פריצה? לא במחשב שלי!

- שמור על המידע במחשב שלך מפני מציצים, מרחרחים, מרגלים, גנבים והאקרים
- מחק את עקבות פעולותיך במחשב בכלל ובאינטרנט בפרט
- סגור את הפרצות באבטחת המידע במחשב האישי שלך.



ייעוץ ועריכה מקצועית:
צור ריכטר-לוין





פריצה?
לא במחשב שלי!

הוראות התקנה והפעלה של התקליטור
בנספח ג' ובקובץ ONCD בתקליטור

עורך ראשי: **זהר עמיהוד**

תרגום: **יואב הופמן**

עריכה מקצועית: **צור ריכטר-לוין** 

עריכה לשונית ועיצוב: **שרה עמיהוד, רמה שנקלר**

עיצוב עטיפה: **ישראל מצגר**

שמות מסחריים

הודעה

לשם שטף הקריאה כתוב ספר זה בלשון זכר בלבד. ספר זה מיועד לגברים ונשים כאחד ואין בכוונתנו להפלות או לפגוע בציבור המשתמשים/ות.

- **טלפון: 09-9564716**
- **פקס: 09-9571582**
- **דואר אלקטרוני: info@hod-ami.co.il**
- **אתר באינטרנט: www.hod-ami.co.il**

פריצה?
לא במחשב שלי!

Michael A. Banks







PC Confidential

By Michael A. Banks

Editor: **Z. Amihud**

הוצאת הוד-עמי

לספרי מחשבים בע"מ

ת.ד. 6108 הרצליה 46160

טלפון: 09-9564716 פקס: 09-9571582

info@hod-ami.co.il

הודפס בישראל 11/2000

ISBN 965-361-266-2 מסת"ב

תוכן עניינים מקוצר

תוכן עניינים

פרק 11: ביקור חוזר באינטרנט: תוכנות עזר 171

פרק 12: מבט מהצד השני 193

מבוא



סיכונים והבטחות בקופסה הקטנה

לפני כ- 20 שנה פרחה וגדלה מולנו (ויש אומרים נפלה עלינו) פתאום מהפיכת המידע. היא הגיעה עם הבטחות למשרד ללא נייר, אמצעים יעילים יותר לניהול רשומות, שיפורים בביצוע מטלות יום יומיות, תעבורת מחשב לעבודה במקום נסיעה לעבודה, חדשות מיידיות, ועוד דברים נוספים שאף כותבי מדע בדיוני לא חלמו עליהם.

יחד עם הבטחות אלו הגיעו גם איומים. **זהירות**, הכריזו אנשים, המפלצת המודרנית תגנוב כסף מכיסכם ותיקח לכם את מקום העבודה. מחשבים יעצבו את מחשבותיכם ורגשותיכם. אתם תספקו לממשלה ולעסקים גדולים, נגד רצונכם וללא ידיעתכם, את כל האמצעים לשעבד אתכם. יותר מאי-פעם, דברים חשובים בחייכם יהיו נתונים לכוונות זדון והרס בשגגה. פרטיות תפסיק להתקיים - כל דבר שתעשה, תאמר, או אף תחשוב יתויק בתיק האישי שלך.

תום הפרטיות היה הגרוע בנבואות ואיומים אלה. נאמר לנו, שבתוך עשור עד שניים, כל חיינו יאוחסנו במסדי נתונים אדירים במחשבים גדולים. הם יאספו על ידי יישויות ממשלתיות וארגונים חסרי-פנים, ומסדי הנתונים יבטיחו ששום דבר לא יוכל להיות פרטי.

אולם, לזמן מה נראה שיתרונות והבטחות המחשב שקולות בהרבה כנגד האיומים - איומים שממילא נראו מנופחים מעל לכל פרופורציה. ואכן, עד למחצית השנייה של שנות ה- 90', חששות כמו אלה שתוארו זה עתה שימשו יותר כחומר לעיתונות צהובה וסרטים משעשעים מאשר היו קיימים במציאות.

העתיד (לפחות עתיד מסוים זה), בכל זאת כבר כאן, והוא אינו מה שהיה פעם. למעשה, המציאות לעיתים אף מפחידה מהחששות. כן, פרטיותנו הולכת ופוחתת. עובדות ופרטים אינסופיים עלינו, מסטטיסטיקות חיוניות דרך רישום אירועים בחיינו ועד לטעמנו באוכל ובידור, אכן מאוחסנים במסדי נתונים ענקיים. אנו במעקב בכל פעם שאנו משתמשים בכרטיס אשראי, מזמינים מוצר, מקבלים טיפול למחלה או פציעה, יוצרים הידברות עם בתי משפט ויישויות חוקיות אחרות, או משנים כתובת. מערכות איסוף מידע שאינן יודעות שובע, אורבות לנו בכל פינה ורושמות את מעשינו.

אך בכל זאת, הן אינן יודעות הכל, נכון? מחשבותינו נשארות פרטיות, יחד עם תכתובות, שיחות, ודברים רבים שאנו עושים לשם בילוי, השכלה, או לשם יישום מטרות קריירה חדשות או תוכניות אישיות כשאנו לבד ואיש לא מסתכל בנו.

לרוע המזל, זה לא בדיוק נכון. למעשה, האיומים עתה אישיים יותר. בנוסף למיגוון האמצעים שיש לממשלה ולחברות גדולות לאסוף מידע אודותינו, היום גם ארגונים קטנים יותר ובודדים יכולים ללמוד עלינו דברים ללא ידיעתנו.

מי הם בדיוק אותם ארגונים ובודדים? הם יכולים להיות כל אחד, מהמפקח שלך בעבודה ועד לשכניך, חברים, או קרובים. במקרים מסוימים, אנשים זרים לחלוטין יכולים לחדור לענייניך האישיים ביותר. גרוע מכך, לא נדרשים אמצעי היי-טק ומעקב מתוחכמים; ניתן לאסוף מידע דרך המחשבים בהם אתה משתמש בבית ובעבודה.

האם באמת ניתן לאסוף מידע מהמחשב האישי בקלות כזו? האם עליך לחשוש ממה שימצא על המערכת שלך? כן, **וכן!**

אלה החיים שלך

איך יכול להיות? אדגים זאת, באמצעות טיול מהיר במחשב שלך בבית ובעבודה.

הנה מכתב ההטפה שכתבת לאחיך לפני שישה חודשים. זוכר? שקלת שנית את המכתב והחלטת לוותר ולא לשלוח אותו. אך המחשב שלך לא ויתר - ואף שלא שמרת או הדפסת את המכתב, ראיתי אותו במחשב שלך! תאר לך שאחיך היה זה שמדפדף במערכת שלך ולא אני.

ומה זה? - אמרת לכולם שלא שמעת **ממנה** כמעט שנה - אך הנה דואר אלקטרוני לוהט שקיבלת ממנה לפני שבוע (ודאי שמחקת אותו, אבל הוא כאן). וזה עוד כלום - תראה את התשובה שהחזרת לה! תפסיק להסמיק. איש לא יוכל לשים את ידיו על זה - או אולי כן?

וואו! יש פה עוד הרבה יותר על מערכת יחסים זו ועוד על דברים נוספים, אך איני רוצה להביך אותך שלא לצורך אז נעבור עתה למעשיך בעבודה. אני בטוח שהמחשב שלך יוכיח שאתה עובד מסור.

הנה הגענו למקום העבודה שלך. אופס! הסתכל בתמונות אלו. לא היית רוצה שראש המחלקה שלך יידע עליהן. כן, אני מאמין לך שביקרת באתר אינטרנט זה בטעות ושלא הורדת כלום ממנו - אך האם המנהל שלך יאמין לך? ומה בדבר הבחור במחלקה השנייה? המציאות המרה היא שאינך צריך להוריד מאומה מהאינטרנט כדי שזה יימצא במחשב שלך.

מה עוד עשית? הנה משהו ראוי לשבח: בהתאם לתיבת המאפיינים המתלווה למסמך פתוח זה, השקעת בדיוק 18 דקות השבוע על דוח פרויקט זה שכבר הנך מפגר בלוח הזמנים להגשתו.

נתקדם הלאה ונעבור על שאר עקבותיך לשבוע זה. הקפדת למחוק את כל הקבצים **האלה?** לא משנה; השארת עקבות. הסתכל בתפריט זה. לפיו, עבדת על מכתב ל**מדריך הטלוויזיה**, תכננת חופשה, ערכת תמונות משפחתיות, ועדכנת את קורות חייך היום **וגם** אתמול.

הנה הגיליון האלקטרוני של הוצאותיך, **בשתי** גירסאות! נראה לי כמו מדע בדיוני. והנה - עוד קבוצת דפים משעשעים בהם ביקרת באינטרנט, לפי רישומי Internet explorer ו-Netscape!

טוב, אני אפסיק. אך הבנת את הרעיון: כל אדם היכול לשים ידיו על המחשב שלך יכול ללמוד עליך הרבה יותר משהיית רוצה שיידע. כל הנדרש הוא מעט זמן והידע המתאים. אף אם לא היה לך מה להסתיר, האם היית רוצה שלמישהו תהיה גישה כה רבה לחייך?

מה בדבר המעסיק שלך, אחיך, חברים, ילדיך, או כל אדם משמעותי אחר? האם תוכל למנוע מהם גישה למחשב שלך?

לא? ובכן, קרא הלאה....

פעולות מזיקות

פן נשכח, יש גם אפשרות שהמידע שלך יימחק, או ייפגע על ידי אדם אחר. ונדליזם או פעולות תמימות יכולים לגרום להרס נתונים שלא גיבית או הדפסת.

מעקב אחרי עניינים פיננסיים, היסטוריים, או אישיים באמצעות המחשב האישי, הוא כה קל עד שאנו שוכחים שהנחנו את כל הביצים בסל אחד. כך אנו מסכנים הכל בפעולת זדון אחת בודדת או שגויה.

איומים מקוונים

כמעט לכל חלק של העולם המקוון יש מקבילים בעולם האמיתי. ניתן לערוך קניות, לתקשר, לבצע פעולות בנקאיות, מחקר ועוד. גם ניתן לרמות אותך בצורה מקוונת, להטריד, לעקוב ואף גרוע מזה.

איומים מקוונים כרוכים לרוב במידע. אפשר למזער את האיום - ואף לבטלו אם תקפיד לשלוט על המידע שלך, כלומר עליך לשלוט על המידע היוצא הנוגע לך. זה כולל, במקרים מסוימים, את דעותיך, כמו גם את זהותך, מספרי כרטיס אשראי, עיסוק, מיקום ועובדות אחרות.

מדוע ספר זה?

כיון שמידע אישי הוא כה יקר ערך ופגיע, וכיון שפרטיות היא שיקול קריטי, הגיע הזמן למדריך פרטיות למחשב בבית ובעבודה. לכך מיועד ספר זה, בו נדריך אותך כיצד לשמור את המידע הפרטי ואת פעילות המחשב שלך פרטיים.

תלמד מה נמצא בסיכון וכיצד למנוע סיכון זה. לדוגמה, תלמד כיצד למנוע מאחרים בעלי גישה למחשב שלך לראות מה כתבת בדואר אלקטרוני ומסמכי Word, וכו׳; מה ביצעת ב-Excel ויישומים אחרים; ובאיזה אתרים ביקרת באינטרנט.

ואולי הבשורה הטובה ביותר היא שתוכל להגן על פרטיותך ללא כלים מיוחדים או מידע טכני. זהו ספר למשתמש מחשב ממוצע ולא לגאוני מחשבים. לצורך כך, אדגים מיגוון טכניקות והגדרות שבהן תוכל להשתמש כדי להגן על הנתונים שלך, ולהימנע מהשארת עקבות שבאמצעותן יוכלו לשחזר את פעילותך הממוחשבת. נראה גם היכן יישומי מחשב כגון Word, Internet explorer, ו-Netscape שומרים העתקי עקבות מוסתרים נוספים וכיצד להיפטר מהעתקים אלה. בנוסף, תלמד על כמה תוכנות שימושיות שיכולות לסייע בכל האמור לעיל.

כלי חיוני נוסף שתרכוש מקריאת ספר זה, הוא הידע לקדד ו/או להגן באמצעות סיסמה על מידע ותוכנות חיוניות. בנוסף, תגלה כמה טכניקות תוכנה המסייעות להגנה על המערכת שלך מפלישת תוכנות וירוס וסוסים טרויאניים וממחיקת נתונים בזדון או בשוגג. כמו כן תגלה כיצד לשמור על פרטיות בדואר אלקטרוני ובאינטרנט.

חטטנים כמונו?

אולי עלה בדעתך, שתוך כדי לימוד כיצד להגן על המידע שלך, ספר זה גם מקנה לך ידע כיצד למצוא מידע חבוי ומוגן במחשבים של אחרים. מה שתבחר לעשות במידע שרכשת בספר זה (מעבר להגנה על הנתונים שלך ופרטיותך), תלוי בך. אם אתה מרגיש צורך "לבדוק" מחשב של מישהו אחר, אתה ודאי תדע כיצד לעשות זאת. אך חשוב לפני שתחטט; אולי לא תאהב מה שתמצא, ואולי תגלה שאתה מתעסק עם מישהו היכול להחזיר מלחמה ביעילות גדולה משלך.

כיצד להשתמש בספר זה

הדרך הטובה ביותר להשתמש בספר זה היא פשוט לקרוא אותו. אך אינך צריך להתיישב ולקרוא את הספר כולו. אם אתה כמו רוב משתמשי המחשב, יש לך בוודאי שאלות מוכנות על מצבים או תוכנות מסוימות. אם זהו המצב, דלג לפרקים הדנים בעניינך. אולי תרצה לרפרף בפרקים לקבלת עצות שימושיות ומעניינות, או שתוכל לקרוא כל פרק ולעבור לבא כשתרצה.

בכל גישה שתנקוט, אני ממליץ לקרוא את פרקים 1 ו- 2 קודם. אחר כך - אתה אדון לעצמך - אך אני ממליץ שתקדיש זמן לניסוי העצות והתחבולות בספר. יישום העצות יחזק את ידיעתך כיצד המחשב עובד ויהפוך אותך למשתמש מיומן יותר.

כמו כן, שמור ספר זה נגיש כמדריך לפרטיות ואבטחת המחשב. אולם, לא תרצה להחזיקו קרוב למחשב, פן מישהו ישתמש בו כדי לגלות על מה הגנת! דפדף גם בתקליטור המצורף, כיון שהוא כולל מספר תוכנות שיסייעו להגנת פרטיותך.

מבנה הספר

בתחילת כל פרק יש רשימת נושאים. זוהי סקירה של הנושאים העיקריים הנידונים בפרק. השתמש בזה כמנחה-מהיר לפרק, וזכור שקיימת גם התייחסות לנושאים קרובים בתוכנם בפרק.

במהלך הספר תראה טקסט מובלט של עצות, הערות, אזהרות, והצללות כמפורט מטה.

זו היא דוגמה להערה. היא מפרטת או מאירה עניין או נושא הנידון בטקסט הסמוך.

זו היא דוגמה לעצה. כאן תמצא עובדות-מהירות ומידע על ביצוע פעולות.

היזהר כשאתה רואה הערה כזו. היא מהווה אזהרה על מצב בו תוכל להסתבך על ידי מחיקת מידע יקר ערך - או אף גרוע מזה.

הערה מוצללת

הערה מוצללת מעין זו מספקת דיון מורחב על נושא בטקסט סמוך ו/או חומר קשור. ראית יישום הערה מוצללת בהקדמה תחת הכותרת "חטטנים כמונו".

בנוסף, הערה מוצללת עשויה להציג סיפור מאיר עיניים או חומר רקע מעניין שלא קשור ישירות לחומר הנידון.

כמו כן, השתמשנו ב**הדגשה (Bold)** לפקודות או טקסט שיש להקליד. כתב **מודגש** משמש להדגיש או להאיר מילה או ביטוי המוגדרים בספר.

נתקדם הלאה

אני מקווה שתמצאו ספר זה מועיל ואולי אף מעט משעשע. אם גיליתם שגיאות או השמטות, או אם יש לכם עצות, אנא שלחו לי הודעה לכתובת:

info@hod-ami.co.il

עתה הגיעה העת לשמור על הנתונים שלך ופרטיותך!

התקליטור המצורף

בתקליטור המצורף תמצא אוסף של תוכנות המיועדות להגן על פרטיותך ועל הנתונים במחשב האישי שלך.

ראה פרטים בנספח ג'.

פרק 1



מדוע לטרוח עם אבטחה? איומים על מערכת ההפעלה, על הנתונים שלך ועליך

מה בפרק:

- ערך ופגיעות המידע
- מה נתון בסכנה
- חטטנות והרס נתונים
- איומים מקוונים
- אסטרטגיות להגנת המידע והפרטיות

מטרת פרק זה היא להציג בפניך את חשיבות המידע והפרטיות בחיים המודרניים, ואת האיומים למידע ולפרטיות הקיימים, לרוע המזל, ממש בתוך המחשב האישי שלך.

רק מחטט?

לפני שנתחיל להגדיר מה הוא מידע ומה ערכו, כדאי שנברר איזה מידע רגיש נמצא "בסכנה". אם תאפשר לי שעתיים עם המחשב הביתי או המשרדי שלך אני עשוי לגלות, בין השאר:

- קבצים אחרונים שעבדת עליהם.
- הודעות דואר אלקטרוני שקיבלת ואולי גם אלו שמחקת (כן, מחקת!) .
- דואר אלקטרוני שכתבת ושלחת.
- אתרי אינטרנט שלמים (כולל גרפיקה) שביקרת בהם.
- משפטים ופסקאות שמחקת ממכתבים או מסמכים אחרים - הם עדיין שורדים אף שמעולם לא הדפסת או שמרת אותם (היכן הסיכון? אולי הערת הערות בוטות או הכנסת מידע רגיש במסמך ואחר כך התחרטת).
- עקבותיך המקוונים היום-יומיים, כולל קבצים שהורדת (אף אם מחקת אותם).
- תאריכים ושעות מדויקות בהן השתמשת במחשב, כולל מידע על מתי וכמה זמן (או כמה מעט זמן) עבדת על פרויקט כלשהו.
- מקורן של רבות מהתוכנות שלך - האם הן נרכשו כחוק על ידך, או הועתקו/הושאלו ממישהו אחר.

כל המידע הזה ויותר ניתן להשגה ללא ידע טכני נרחב או כלי תוכנה ייחודיים. מקורות הסיכון רבים: עמיתים לעבודה, מפקחים, עובדים, בני/בנות זוג, שותפים, ילדים, חברים, אויבים - כל אחד יכול לדעת על פעילותך המקוונת והלא מקוונת הרבה יותר משחשבת.

אם אתה חושב שאין לך מה להסתיר, שקול את הדוגמאות הבאות על אנשים שנבגדו על ידי המחשבים שלהם:

- שוטרת מחקה בקפידה מהמחשב במקום עבודתה דואר אלקטרוני אישי המתייחס לחיפוש עבודה - אך היא ננזפה על שימוש לא הולם במערכת המחשב בשעות העבודה, כיון שבתפריט **התחלה, מסמכים** נמצאו שני מסמכים עם קורות חייה.
- גבר מצא את עצמו בהליכי גירושין כיון שאשתו גילתה במקרה כמה מכתבים לחברה "מיוחדת" - מכתבים שמעולם לא שמר בדיסק. מכתבים אלה היו בעלי כוונות תמימות, אך מהסוג הניתן לפירוש לא נכון - ואכן כך פורשו.
- אישה גילתה שכל ההיסטוריה הפיננסית שלה פתוחה בפני חבר שהשתמש במחשב שלה לעיבוד תמלילים.
- סטודנט העיר כמה הערות "לא נבונות" בפורום באחד האתרים באינטרנט - הערות שהפריעו לו שנתיים מאוחר יותר, כאשר פנה לקבלת עבודה בארגון גדול.
- שני ISPs (ספקי אינטרנט) סיפקו למשטרה מידע רב על הזמן, המקום, ושם הנער שהשתמש במספר של כרטיס אשראי גנוב, לצפייה בפורנוגרפיה מקוונת.

פרט לאישה שהמידע הפיננסי שלה נפרץ, לא ניתן להגיש תביעות כלשהן במקרים אלה על פגיעה בפרטיות. יומני תעבורת אינטרנט הם ששימשו בתיק התביעה של כרטיס האשראי הגנוב, ובמקרים אחרים, אנשים נתקלו במידע באקראי, תוך כדי שימוש שגרתי במחשב משותף (לא נעשה כל מאמץ מיוחד לעיין במידע בכוונה).

הנקודה היא שמידע שיחק תפקיד מכריע בכל אחת מהדוגמאות. בכל מקרה (פרט להיסטוריה הפיננסית) ערך המידע ניכר רק לאחר שנפרץ - בסך הכל דוגמאות אלו מעידות על העובדה שערך הוא דבר יחסי.

ערך המידע

מידע מניע כמעט כל דבר בתרבות המערבית בת זמננו, וכמעט דבר אינו מתרחש ללא המידע המתאים. לדוגמה, כאשר אתה רוכש כרטיס טיסה ומשלם באמצעות כרטיס אשראי, מידע אודותיך נאסף (להיכן טסת, מתי, באיזה סוג כרטיס אשראי השתמשת ועוד...). דבר זה נכון גם כאשר אתה מגיש בקשת הלוואה לרכישת רכב או בית, מקבל מרשם, או מתחבר לשירותי טלפון, חשמל או מים. בכל פעולה כזו, המידע נאסף. בנוסף, מידע חדש נוצר ונשמר.

אותו מטוס עבורו רכשת כרטיס טיסה? הוא לא עוזב את השער ללא מידע - על מזג האוויר, הנוסעים, הצוות, והמטוס עצמו. כך גם בהובלות - ברכב, רכבת, מטוס, דואר, או שליח - ההובלות אינן מתבצעות ללא תעבורת מידע רבת היקף.

יש מעט מאוד דברים הניתנים לביצוע בעולם המודרני שאינם כרוכים באיסוף, שיתוף, יצירה, או גישה למידע. הכפל את המידע הכרוך בדברים שאתה עושה בכל יום נתון, (קנייה, השכרה, עשיית מנוי, הזמנה, לקיחת הלוואה, תשלומים, מתן הלוואה, נסיעות, הגשת בקשה), בכמה מאות מיליוני אנשים, וקל לראות שסך כמות המידע הכרוכה בכל זה היא מדהימה.

מידע הוא דבר **יקר ערך**. כה יקר, למעשה, שחלק נכבד בכל ענף - כולל עסקים, מחקר, תעשייה, וממשל - מיועד לאיסוף, עיבוד, מיון ואחסון מידע. אספקת גישה למידע היא פעילות עסקית גדולה בפני עצמה.

מה, אם כן, הוא ערך המידע? לעיתים, הערך הוא סכום קבוע (הנקבע לרוב באופן שרירותי), כגון $500 עבור השמות והכתובות של עשרת אלפים איש הקונים סוג מסוים של מוזיקה. אולם, לעיתים, ערך המידע הוא סובייקטיבי. לדוגמה, אם אתה יודע שאדם שאינך מכיר מתכנן גירושין או עסקה גדולה או שינוי קריירה מידע זה חסר ערך עבורך. אולם, לאשתו של אותו אדם, לשותפו העסקי, או לעובדיו, מידע זה יכול להיות בעל ערך רב מאוד. למעשה, הוא אפילו בעל ערך רב יותר לאדם עצמו, הרוצה לשמור אותו בסוד.

מידע ופגיעות

בחלק זה נתייחס לשני סוגי המידע - זה בעל הערך הסובייקטיבי, וזה בעל הערך האובייקטיבי - ונוודא שמידע אישי אכן יישאר אישי ופרטי.

מה המחיר של חשיפת מידע אישי?

עבור אנשים מסוימים חשיפת מידע פרטי עלולה להיות בעלת תוצאות אישיות הרסניות. לדוגמה, אם מנהל רשת מחשבים מעיין בדואר אלקטרוני של העובדים באופן אקראי, ומגלה רומן סוער בין שני עובדים (בסביבת עבודה בה נאסר קיום קשרים כאלה בין עובדים), חשיפת התכולה של הדואר האלקטרוני עלולה ליצור בעיות לשני העובדים המעורבים - בבית ובעבודה. בדומה, אם מנהל הרשת גילה תכתובת הדנה בהצעת עבודה של חברה מתחרה לעובד, חשיפת מידע זה עלולה לעלות לעובד במשרתו (אגב, מנהל הרשת אינו מפר חוקי פרטיות כלפי אף צד. בהתאם לתקדים, מידע הנוצר על מחשב החברה, בשעות העבודה, הוא "רכוש" החברה).

אולם, עצם העובדה שדבר שאינך רוצה שייוודע כן נודע, הוא דבר מתסכל ומרגיז. בכל מקרה, כאשר חטטן משיג מידע שאינך רוצה שיהיה בידי איש, זוהי לכל הפחות פלישה לפרטיות.

מה בדבר השמדה או שינוי מידע?

הרס נתונים הוא כבר עניין אחר. אם נתונים נעלמו, הם נעלמים לצמיתות, אלא אם כן אתה שומר גיבויים (על דיסקט או עותק מודפס). לעיתים ניתן לשחזר נתונים, אך תוך השקעת זמן ומאמץ (ואולי כסף) רב ותמיד נשאר הספק אם הכל שוחזר, והאם מה ששוחזר - תקין.

אי-הגנה על מידע: מה הסיכון?

האם זה באמת כל כך נורא? האם מישהו יכול לקבל כל כך הרבה מידע מהמחשב שלי שעלי להרגיש מאוים? כן, וכן.

מה עוד, שלא נדרשת תוכנה או חומרה מיוחדים, כך שבמאמץ קטן, כל אחד יכול להשיג מידע עליך ולדעת מה אתה עושה במחשב . חטטן עקשן יכול לראות מה עשית במחשב בעבודה ובבית. אדם זה יכול אפילו לדעת מתי השתמשת במחשב של חבר או במחשב בספריה, כיתה, או בכל מקום אחר.

חשוב על הדברים שאתה עושה במחשב היכולים להשאיר עקבות או להצביע על מידע שלא נוח לך לשתף, או העשוי להשאיר רושם מוטעה. חשוב על כך עתה, ולא תצטרך לדאוג לכך מאוחר יותר.

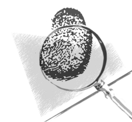
עליך לנקוט באמצעים הנדרשים כדי להגן על המידע שלך.

הרס נתונים

בנוסף לחטטנות, קיימת גם אפשרות שמישהו יהרוס קבצים והגדרות חשובות במחשב. זה יכול להיעשות בזדון או בטעות (כן, דברים כאלה קורים; ראיתי מספר מקרים של מחיקת קבצי מערכת הפעלה על ידי ילדים או מבוגרים "שהלכו לאיבוד" בעת שימוש במחשב והחלו לנסות כל דבר שניתן ללחוץ עליו עם העכבר).

הנזק אינו מוגבל רק לקבצים מחוקים. ונדלים יצירתיים יותר עלולים לבצע שינויים קטנים ובלתי מורגשים בקבצים כדי ליצור בעיות. למשל ניתן להרוס ערך שם/כתובת/מספר טלפון במסד נתונים על ידי שינוי ספרה אחת או שתיים או אות בכל רשומה.

וכאילו לא די בכך, ישנם גם וירוסים וסוסים טרויאניים. חלקם "שקטים" בדרך שהם משנים או מוחקים דברים במערכת, וחלקם בוטים. בשני המקרים, פעילותם מציקה במקרה הטוב וטראגית במקרה הגרוע (פרק 8, **הגנה מפני וירוסים**, דן ביתר פירוט בתוכנות וירוסים וסוסים טרויאניים).



אני אחזור על עצה זאת בפרקים הבאים, אך עליך לדעת שההגנה הטובה ביותר נגד וירוסים וסוסים טרויאניים היא להכיר את מקור המידע. אם מישהו נותן לך דיסקט ממקור לא ידוע, אולי עדיף לא להריץ אף תוכנה שהוא מכיל. אם אינך בוטח באתר אינטרנט או בשירות מקוון שממנו אתה מוריד חומר, אל תוריד מאומה.

לרוב, ניתן לטפל בסיכון שבהרס או מחיקת נתונים על ידי תכנון מראש ונקיטת אמצעים מתאימים.

איומים מקוונים

המקור הנפוץ ביותר לוירוסים וסוסים טרויאניים, הוא האינטרנט. קבצים שהורדו עלולים להיות מסוכנים, אך הם אינם האיום המקוון היחיד בו אתה עלול להיתקל. לעיתים קרובות, האיום הגדול ביותר הם אנשים.

תחת מעטה האנונימיות, אנשים עושים לעיתים דברים שלא היו עולים בדעתם אחרת. האינטרנט הוא מקום לכל מיני רמאויות ושרלטנים, בנוסף להטרדות, מעקבים, גניבה אמיתית, ועוד.

מעט מידע יכול לעשות צרות גדולות בעולם המקוון. אם אדם מקוון בעל כוונות זדון ישיג מעט מידע עליך, הוא יוכל לגרום לך צרות רבות, מקוונות ולא מקוונות. עם הידע המתאים, תוכל לרוב להימנע מבעיות מקוונות ולהעלים כמעט כל בעיה שצצה.

אולם, הבעיות אינן נפסקות כאשר אתה מתנתק. דפדפן האינטרנט עלול לשמור רישומים מדויקים להפליא על פעילותך באינטרנט. גם מה שהורדת עלול להירשם. תוכנית הדואר האלקטרוני ואפילו ספק האינטרנט שלך עלולים ליצור עקבות שחטטן מיומן יוכל לעקוב אחריהן. למרבה המזל, ניתן להעלים עקבות אלה על ידי שינוי הגדרות ומחיקות נבונות, כמתואר בפרק 6, **כיצד למנוע מקבציך להסגיר אותך**, פרק 9, **ביטחון ופרטיות באינטרנט** ופרק 10, **הגנת דואר אלקטרוני**.

אסטרטגיות להגנת המידע והפרטיות

בעולם המקוון או הלא מקוון, הגנת המידע והפרטיות מסתכמת בדבר אחד: שליטה על המידע. עליך לשלוט על מקום אחסון המידע, להגביל גישה אליו, ולשמור על שלמותו. האסטרטגיות הבסיסיות כוללות:

- **אבטחת המערכת -** מתי והיכן שניתן, הגבל את מורשי הגישה למחשב שלך, בעבודה ובבית. היעזר לשם כך בסיסמה, ובאמצעי אבטחה נגד תוכנות מיד-שנייה העלולות להכיל וירוסים או סוסים טרויאניים (ראה פרק 2, **לוגיסטיקה ותחבולות בסיסיות לאבטחת המחשב**, ופרק 3, **פשוט וישיר - הגנת המידע באמצעות סיסמאות והגדרות**).
- **הסתרת מידע -** אם איש מלבדך אינו יודע היכן אחסנת את המידע, סכנת החדירה לפרטיות או הרס המידע יקטנו. לצורך כך, השתמש בתחבולות כמו שמות מטְעים לקבצים או קבצים ותיקיות "בלתי נראים". עליך גם למחוק את כל העקבות לנתוניך, בין השאר, על ידי מחיקת רישומים בתפריטי קבצים ומסמכים ב-Windows (פרק 3, **פשוט וישיר - הגנת המידע באמצעות סיסמאות והגדרות**, פרק 4, **הגנה על קבצים ותיקיות באמצעות הסוואה והטעיה**, פרק 5, **הסתרת קבצים, תיקיות, ויישומים**, פרק 7, **הצפנת מידע** ופרק 10, **הגנת דואר אלקטרוני**).
- **הגנה על מידע מהרס/שמירת שלמותו -** כאן, העניין הוא מניעת מחיקה, שינוי, או הרס המידע. לצורך כך, טקטיקות כמו גיבוי נתונים, נעילת קבצים, והגנה באמצעות סיסמאות הן יעילות ביותר (פרקים 2, 3, 4, 5, 8, **הגנה מפני וירוסים**, ו- 11, **ביקור חוזר באינטרנט: עזרי תוכנה**).

- **הסרת מידע מאזורים נגישים -** כאשר מדובר במידע רגיש ביותר, ייתכן שהסתרה ונעילת קבצים אינה מספיקה. תצטרך ליישם טקטיקות כגון שמירת קבצי עבודה על דיסקטים, או שמירת נתונים כפלט מודפס בלבד. כמו כן תצטרך גם למחוק גיבויים שבוצעו על ידי מערכת ההפעלה (פרקים 3, 4, ו- 5).
- **העלמת המחשב שלך ממעגל המידע -** הקדש מעט מחשבה אם באמת רצוי ליצור ולשמור סוגים מסוימים של מידע במחשב (פרקים 2, 3, 5, ו- 7, **הצפנת מידע**).
- **מחיקת עקבותיך -** Windows ויישומים אחרים הם כפייתיים ביותר בשמירת עקבות מעשיך בהפעלות האחרונות שלהם. תוכל להעלים את רוב העקבות באמצעות הגדרות; את השאר ניתן להעלים ידנית (פרקים 2, 3, 6, 10 ו- 11).

טקטיקות

החלת האסטרטגיות המוזכרות לעיל דורשת שתנקוט באמצעי זהירות מסוימים, לפני ואחרי יצירה, גישה, או אחסון מידע במחשב שלך.

חלק מהטקטיקות ייעודיות ליישומים מסוימים; אחרות כרוכות ב-Windows עצמה ו/או כיצד אתה מטפל במידע. הפרקים הבאים מפרטים את הטקטיקות הנדרשות. אנו נתחיל בהתחלה כמובן, ונדון בבסיס בפרק 2. שם תמצא מידע שימושי על מיקום המחשב וציוד היקפי, מחיקת קבצים מיותרים העלולים ליצור בעיות אם חטטן מאתר אותם, עשיית גיבויים, ונקיטת אמצעי זהירות בעת עזיבת המחשב.

פרק 2



לוגיסטיקה ותחבולות בסיסיות לאבטחת המחשב

מה בפרק:

- *הצבת מערכת המחשב במקום בטוח*
- *הדפסה או העתקת דואר אלקטרוני רגיש*
- *מחיקת קבצים לצמיתות*
- *גיבוי קבצים*
- *אבטחת המידע ומערכת ההפעלה בעת עזיבת המחשב*
- *בדיקת המחשב לאחר היעדרות*
- *מחיקת עקבות מתפריט המסמכים*
- *נקיטת אמצעי זהירות בעת כיבוי המחשב*

פרק זה דן בנושאים בסיסיים רבים, אשר ייראו מובנים מאליהם לחלק מהקוראים. ובכל זאת, רצוי להתחיל בהתחלה, באמצעים הנפוצים והפשוטים ביותר להגנת הפרטיות והמידע. יש להניח שתמצא כאן כמה תחבולות שלא עלו בדעתך.

לאלה מכם החדשים לעולם המחשבים, פרק זה נועד להתניע אתכם. הוא כולל עצות וטכניקות בהן תוכלו להשתמש מייד, ללא כל ידע נוסף או תוכנות נוספות.

מי מסתכל מעבר לכתפי?

אחד מאמצעי האבטחה הברורים והמוזנחים ביותר הוא מיקום המחשב. רובנו מציבים את המחשב במקום הנוח ביותר. אנו חושבים במושגים של מקור מתח זמין, המקום הטוב ביותר על המכתבה או השולחן, וכן הלאה. אולם, אם אתה מייחס חשיבות לאבטחת פעילותך במחשב, קח בחשבון שכל אדם במקום העבודה או בביתך יוכל לראות בדיוק מה אתה עושה פשוט על ידי צפייה במסך.

ניטור המסך

כיון שכל אדם יכול לעבור לידך ולראות מה אתה עושה על ידי צפייה במסך, בין אם אתה נוכח או לא, עליך לשקול את מיקום המסך. המקום הטוב ביותר - שאולי ייראה מובן מאליו - הוא כאשר הכסא שלך מוצב כך שגבך לקיר והמסך פונה אליך. בצורה כזו, איש לא יוכל להסתכל מעבר לכתפך או לצפות בדרך אחרת במסך, אלא אם תרצה בכך.

ייתכן שהזזת דברים במקום העבודה אינה אפשרות קיימת, אך תוכל לנסות להסתיר את המסך ממבט צד באמצעות תיק או עצם גדול אחר. הקפד שהעצם המסתיר ייראה כאילו הוא שייך לשולחנך; אחרת, תמשוך תשומת לעובדה שאתה מנסה להסתיר משהו.

הרבה רעש על לא כלום?

בחברת Start-Up הגיעה הוראה, שאין להפנות את צגי המחשב לעבר החלון. זה נראה די קיצוני, אך כולם שיתפו פעולה והיו עסוקים בסידור מחדש של השולחנות והמחשבים.

לאחר מכן, התבקשו כמה מהעובדים לצאת, מצוידים במשקפת רבת עוצמה, למגרשי החניה, לטפס על גגות הבניינים הסמוכים ולנסות לקרוא את מה שהופיע על המסכים. אם העובדים יכולים לקרוא צגים מנקודות אסטרטגיות סביב הבניין, גם מרגלים תעשייתיים הנשלחים על ידי המתחרים בוודאי יוכלו לעשות זאת.

אל תשמור - הדפס!

גם מדפסות מאפשרות חדירה לפרטיות. הצב את המדפסת כך שהפלט אינו זמין לצפייה. אם אתה עובד בסביבת רשת בעלת מדפסת משותפת, האבטחה הטובה ביותר היא לשלוח רק חומר חוקי להדפסה.

מדפסת משותפת

פרופסור באוניברסיטה שהדפיסה באופן שגרתי על מדפסת משותפת במחלקה שלה. המדפסת הייתה במרחק מספר חדרים ממשרדה, כך שלא היה לה מושג מי רואה את מה שהדפיסה. היא מעולם לא הקדישה לכך מחשבה - עד שמישהו שאל אותה בנוגע להדפסת הזמנות למסיבה פרטית. לא נעים.

אם ברצונך להדפיס משהו ויש לך גישה רק למדפסת רשת במקום עבודתך, העתק את הקובץ הנדרש לדיסקט והדפס אותו באמצעות המדפסת הביתית או בבית דפוס (זכור למחוק את הקובץ מהדיסק הקשיח לאחר שהעתקת אותו).

דואר אלקטרוני

דואר אלקטרוני, בין אם בסביבת רשת או לא, הוא נקודת תורפה לרוב משתמשי המחשבים במקום העבודה. השתמש באמצעי הזהירות להלן:

- ❖ אל תשמור העתקי הודעות ששלחת על הדיסק הקשיח. כך גם לגבי הודעות נכנסות שאינך רוצה שייקראו על ידי אחרים.
- ❖ אם ברצונך לשמור הודעות דואר אלקטרוניות נכנסות, אחסן אותן על דיסקט (אם כבר יש ברשותך כמה הודעות נכנסות ויוצאות, הכנס את כל ההודעות לקובץ אחד, אם תוכנת הדואר האלקטרוני שלך מאפשרת זאת). לחליפין, תוכל פשוט להדפיס את ההודעות. אל תשכח למחוק את ההודעות המקוריות - עוד תגלה שהדואר האלקטרוני שלך במעקב! (הדרך הבטוחה ביותר היא לשמור דואר על דיסקטים, או להדפיס הודעות. אף אם תוכנת הדואר האלקטרוני מציעה הגנת תיקיות באמצעות סיסמאות, יש להניח שמנהל המערכת יכול למצוא דרך לעקוף זאת).
- ❖ ודא שההודעות שנמחקו נעלמו באמת. מחיקת דואר אלקטרוני אינה בהכרח מוחקת אותו. בהתאם לתוכנת הדואר האלקטרוני שברשותך, הודעות מחוקות עלולות פשוט לעבור לתיקיית זבל, שיש לרוקנה לפני שהן יימחקו בפועל (הסעיף הבא דן ביתר פירוט בתיקיית הזבל וסל המיחזור, האחראים לטיפול בקבצים מחוקים).
- ❖ בדוק את סביבת העבודה של המחשב האישי שלך, אם הוא מחובר לרשת. ייתכן שהדואר האלקטרוני שלך מאוחסן על השרת ומגובה, אף שמחקת אותו. מצב זה שכיח ביותר בסביבת רשתות גדולות.

כמובן, שאמצעי זהירות אלה חלים גם על מחשבים ביתיים.

רוקן את סל המיחזור

אולי אינך מודע לכך, אך לפי הגדרות ברירת המחדל ב-Windows, סל המיחזור **מאחסן** קבצים "מחוקים", עד לריקון. ניתן לבטל מחיקת קבצים אלה על ידי פעולת שחזור, או לעיין בהם בעודם בסל המיחזור.

עקב כך, עליך לרוקן את סל המיחזור תקופתית, כדלקמן:

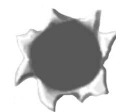
1. פתח את סל המיחזור.
2. בחר **קובץ** ולחץ על **רוקן סל מיחזור** כמתואר בתרשים 2.1.



תרשים 2.1 ריקון סל המיחזור

סל המיחזור יכול לשמש אותך אם ברצונך לשחזר קבצים שנמחקו בשוגג. אולם, אם אתה מעדיף לדלג על סל המיחזור ולמחוק קבצים לצמיתות במקום, עקוב אחר השלבים הבאים:

1. לחץ לחיצה ימנית על סמל **סל המיחזור** בשולחן העבודה.
2. בחר **מאפיינים** מהתפריט המוצג. תיבת הדו-שיח של מאפייני סל המיחזור תופיע, כמתואר בתרשים 2.2.
3. לחץ על כרטיסיה ***כללי***.
4. לחץ על לחצן האפשרויות **אל תעביר קבצים לסל המיחזור. הסר קבצים מייד עם מחיקתם.**
5. לחץ **אישור.**

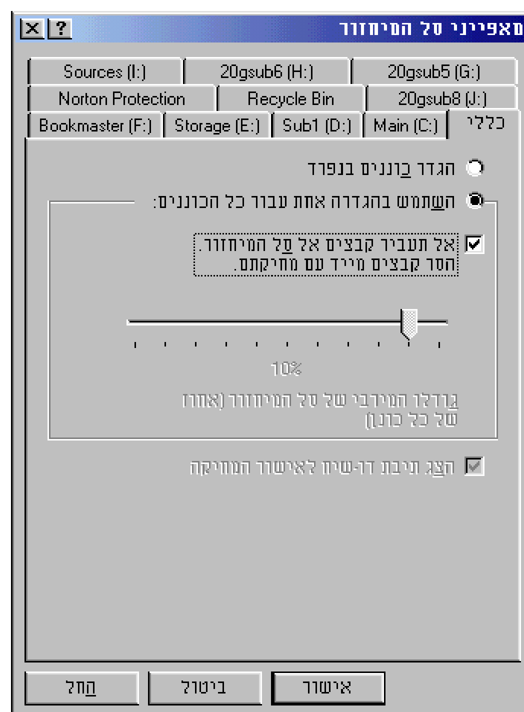


זכור שאם הגדרת את סל המיחזור להסיר קבצים מייד, לא תוכל לשחזר קבצים לאחר מחיקתם.

אתה יכול ליהנות משני העולמות: גם להשתמש בסל המיחזור וגם למחוק קבצים שלא בעזרת סל המיחזור. כדי לעשות זאת, יהיה עליך לבטל את האפשרות **הסר קבצים מייד עם מחיקתם** ממאפייני סל המיחזור.

1. פתח את **סייר Windows**.
2. סמן את הקבצים שברצונך למחוק.
3. החזק את מקש **Shift** לחוץ.
4. לחץ על מקש **Delete** והרפה ממקש **Shift**.

הקבצים שסומנו יימחקו ולא יועברו לסל המיחזור.



תרשים 2.2 הגדרת סל המיחזור להסרת קבצים מייד.

מניעת מחיקות הרות-אסון: גיבוי המערכת

אם אתה חושש שמישהו מוחק קבצים בזדון או בטעות, או אם נכנס וירוס למערכת או שהיא קרסה, יש רק דרך אחת לוודא שתמיד תוכל לגשת לקבצי הנתונים - והיא לגבות את הקבצים.

ייתכן שיצרת **דיסקט הצלה** או **דיסקט אתחול** בעת התקנה והגדרת המחשב. דיסקט הצלה או אתחול הוא דיסקט המכיל את קבצי מערכת ההפעלה הנדרשים לאתחל את המחשב מכונן A, ומעט נתונים על הגדרות המחשב שלך. אחסן דיסקט זה במקום בטוח לשימוש במקרה של כשל דיסק קשיח (לא ליד המחשב).

אולם, לדיסקט ההצלה או האתחול אין כל קשר לקבצי המידע שיצרת באמצעות יישום כלשהו - מעבד תמלילים, גיליון אלקטרוני, עורך גרפי, וכן הלאה - או למידע שהתקבל ממקור חיצוני (כגון הודעת דואר אלקטרוני או קבצים שהועתקו מדיסקט). יש לגבות (להעתיק) את כל קבצי המידע החשובים למדיה חליפית, כגון דיסקטים, קלטת גיבוי, (חלקם משמשים לגיבוי **כל** תכולת הדיסק), או כונן ZIP. גם תקליטורים הם אפשרות טובה לכך, אך רק למידע שאינך מתכוון לערוך או לשנות, כיון שלא ניתן לערוך מידע על תקליטורים מסוג CD-RW.

המדיה בה תשתמש תלויה בתקציב, הרגלי העבודה, ונפח ומספר הקבצים שעליך לגבות.



אם אתה משתמש בדיסקט או דיסק ZIP לגיבוי קבצי נתונים, מומלץ ליצור תיקיות ותת תיקיות על הדיסקט המהווים העתק של התיקיות בהן מאוחסנים קבצי המקור בדיסק. דבר זה מקל מאוד על איתור קבצים מאוחר יותר.

הייה זהיר לגבי מקום אחסון הגיבויים. אחסן גיבויים במקום שלאחרים קשה להגיע, ובסביבה יבשה בטמפרטורה שאינה עולה על 30 מעלות (לא בסמוך למחשב).

דיסקים/דיסקטים חיצוניים ואחסון

אם ברשותך מסד נתונים, גיליון אלקטרוני, מעבד תמלילים, או קבצים אחרים שאינך מעוניין שאחרים יראו, אל תשמור אותם על הדיסק הקשיח של המחשב שלך. במקום זאת, צור או העתק את הקבצים על דיסקט או דיסק ZIP (ואל תשכח למחוק את הקבצים המקוריים אם יצרת ו/או עבדת עליהם בדיסק הקשיח).

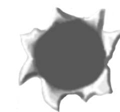
הערה מיוחדת לאלה מכם העובדים בסביבת רשת: בין אם אתה מודע לכך או לא, קבצי העבודה שלך נשמרים בשרת החברה - ולכן ניתן לגשת אליהם. אם ברצונך לעבוד על קבצים אישיים במקום העבודה, השתמש בדיסקט כדיסק העבודה שלך. צור ושמור קבצים הדרושים לך על דיסקט זה בלבד.

אם אתה משתמש בדיסקט 3.5 אינץ' סטנדרטי וקבציך גדולים מאוד, תגיע לנקודה בה לא תוכל יותר לפתוח או לשמור קובץ על הדיסקט. במקרה זה, העתק את הקובץ לדיסק הקשיח כדי לעבוד עליו, העתק אותו בחזרה לדיסקט, ומחק את ההעתק שעל הדיסק הקשיח לאחר שסיימת לעבוד עם הקובץ.

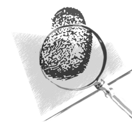


בעת הדבקת תוויות על דיסקטים או דיסקי ZIP המכילים מידע רגיש, שקול שימוש בתוויות מטעות. לדוגמה, במקום לכתוב "מסד נתונים פיננסי" על דיסקט, השתמש בתווית הבלתי מזיקה "מתכונים ישנים". רק זכור את השמות שנתת לקבצים, כך שלא תאבד אותם!

שוב, המקום בו אתה מאחסן את הדיסקטים חשוב במונחים של נגישות ואבטחה.



לאחר העתקת קבצים לדיסקט, ודא שהם אכן על הדיסקט לפני מחיקת הגירסה שעל הדיסק הקשיח. עיין בתיקיית הדיסקט על ידי בחירה בה בסייר Windows, או באמצעות DOS. אם לא תחזור ותבדוק, בסופו של דבר אתה עלול לאבד קבצים.



המדיה של דיסקט, היא מדיה מאוד לא אמינה (לפחות במושגים של היום). היא ניידת וקלה, אבל אמינות זה לא הצד החזק שלה. בהמשך נסקור שיטות חלופיות לאבטחת המידע מאשר העתקתו לדיסקט.

כאשר אתה עוזב את המחשב

כאשר המחשב שלך נמצא ללא השגחה, אחרים יכולים לגשת אליו. להלן מספר עצות כיצד להפוך את המערכת לבלתי נגישה לאחרים, כיצד לבדוק אם מישהו עשה שימוש במחשב בהיעדרך, ומספר אמצעי זהירות שעליך לנקוט בעת כיבוי המחשב.

שיתוק זמני של המערכת שלך

רובנו לא אוהבים לכבות את המחשב אם אנו עומדים להיעדר מספר דקות בלבד. אולם, אם קיימת סכנה שמישהו יצפה בפעילותך, תמיד ישנה אפשרות של הגנת המערכת כולה באמצעות סיסמה (עיין בפרק 3 ובתקליטור המצורף, המכיל תוכנות הגנה באמצעות סיסמה). אם טרם התקנת תוכנה להגנה באמצעות סיסמה, ישנה אפשרות אחרת, ולעיתים טובה יותר מכיבוי המחשב, והיא לשתק את המערכת זמנית. בכך תקשה על אנשים חסרי ידע בחומרת מחשב להציץ במעשיך, אולם זה לא ימנע חטטנים עקשנים בעלי ידע במחשבים. אך אל חשש, יש עוד תחבולות ועצות להדיפתם בפרקים הבאים.



שיתוק זמני של המערכת יעיל גם אם אתה משתמש במחשב של מישהו אחר, ולא יכול להוסיף תוכנת הגנה באמצעות סיסמה.

אפשרויות השיתוק כוללות:

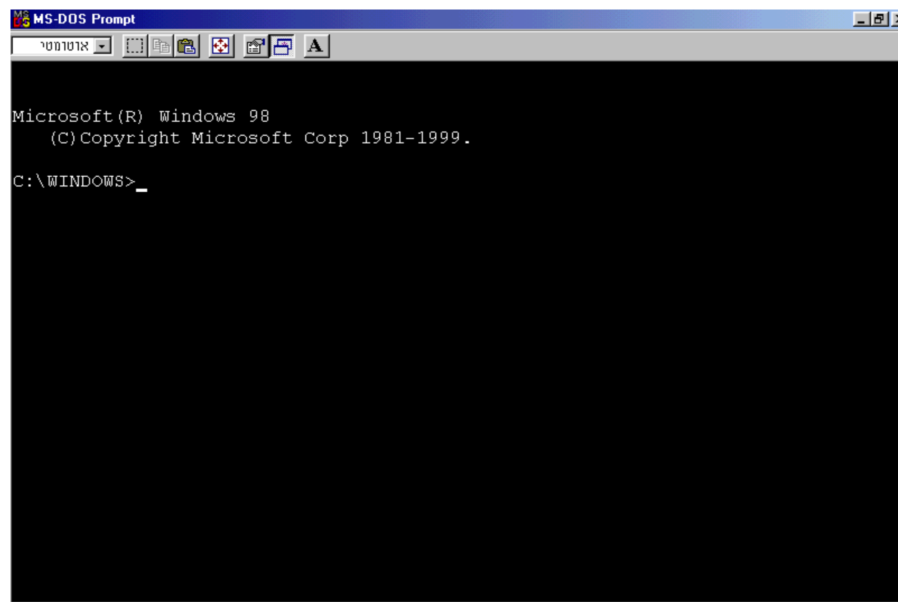
- כיבוי המסך.
- הוצאת תקע כבל המסך (כבל המתח של המסך או הכבל שבין המחשב למסך).
- ניתוק כבלים משקעי המקלדת והעכבר.

אמצעי זהירות אלה יעילים במניעת חדירה למחשב על ידי אנשים חסרי כל ידע במחשבים. כמובן, אם אתה עצמך חסר ידע רב בחומרת מחשבים, לא רצוי שתתעסק עם דברים אלה. אם אכן ניתקת כבל או שניים, החבא אותם או קח אותם אתך.



זכור שגורם ההפתעה הוא גורם מנצח. אם בהיעדרך הגיע לשולחנך, חטטן והמחשב לא "נענה" לו, הוא קודם כל מופתע. לזה הוא לא התכונן ועכשיו הוא יתלבט מה לעשות ואולי יחליט לעזוב את המחשב שלך ולסגת לפני שייתפס.

פתרונות תוכנה לבעיית חטטני מחשב בהיעדרך כוללים הגנת מערכת ההפעלה באמצעות סיסמה, כפי שהוזכר קודם, או מעבר ל-DOS-מסך-מלא. אדם חסר ידע במחשבים, בראותו מסך כמוצג בתרשים 2.3, לא יוכל לעשות הרבה - אלא אם כן, הוא יודע מספיק כדי להקליד EXIT וללחוץ על Enter כדי לחזור ל-Windows או לכל יישום אחר הרץ במחשב.



תרשים 2.3 לעיתים, הצגת מסך DOS פשוט, תמנע מסקרנים משועממים לצפות במערכת.

אם כבר מדברים על אנשים חסרי ידע, אם אתה מתאים או קרוב להגדרה זו כמשתמש במחשב, להלן כיצד להגיע למסך DOS המוצג בתרשים 2.3. תחילה, פתח את תפריט **התחל (Start)**, בחר בתפריט **תוכניות (Programs)**, לחץ על **הפנייה ל-MS-DOS**, וזהו, אתה ב-DOS.



אם, לאחר שעברת ל-DOS הוא מוצג בחלון קטן מעל שאר החלונות, לחץ **ALT+Spacebar (ALT + רווח)** לעיון בתפריט חלון DOS. בחר **הגדל** בתפריט זה, ו-DOS יתרחב **וימלא** את כל המסך.

לחזור ליישום אחר ממסך DOS, לחץ **Alt+Tab**. ליציאה מ-DOS לחלוטין, כתוב **EXIT** במנחה שורת הפקודה <:C (C:\WINDOWS>EXIT) והקש Enter.

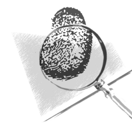
חיפוש עקבות בקבצים

האם אתה נאלץ להשאיר את המחשב עובד בהיעדרך, או אין יכול למנוע מאחרים להפעיל אותו כאשר אתה עוזב? אם כך, תוכל לדעת אם מישהו פתח קובץ מסוים בהיעדרך. להלן דרך מהירה וקלה לבדוק, באמצעות **סייר Windows**:

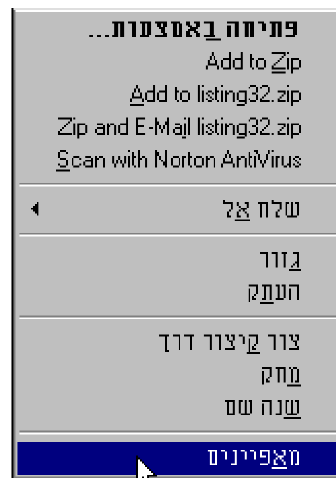
1. התחל את **סייר Windows** על ידי בחירתו מתפריט **תוכניות** שבתפריט **התחל**.
2. נווט לתיקיה בה מאוחסן הקובץ.
3. לחץ לחיצה ימנית על שם הקובץ, ובחר **מאפיינים** מהתפריט המוצג.

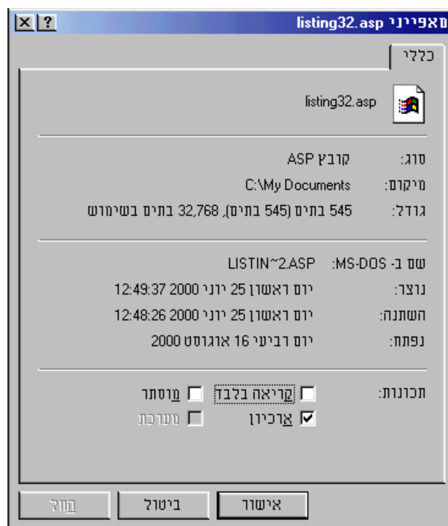
תיבת הדו-שיח **מאפייני קובץ** תופיע כמתואר בתרשים 2.4, ובה קובץ דוגמה בשם Listing 32.asp. במרכז התיבה כתוב מתי הקובץ נוצר, מתי השתנה, ומתי נפתח לאחרונה.

אם התאריך/זמן שבו ניגשו לקובץ זה לאחרונה הוא אחרי שהשתמשת במחשב, מישהו אחר פתח קובץ זה.



תוכל גם לעיין בתיבת הדו-שיח **מאפיינים** על ידי לחיצה ימנית על קובץ מהרשימה הנוצרת כאשר אתה בוחר **פתח** בתפריט קובץ של יישום.

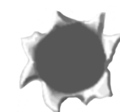




תרשים 2.4 עיין במאפייני קובץ לראות אם מישהו פתח אותו בהיעדרך

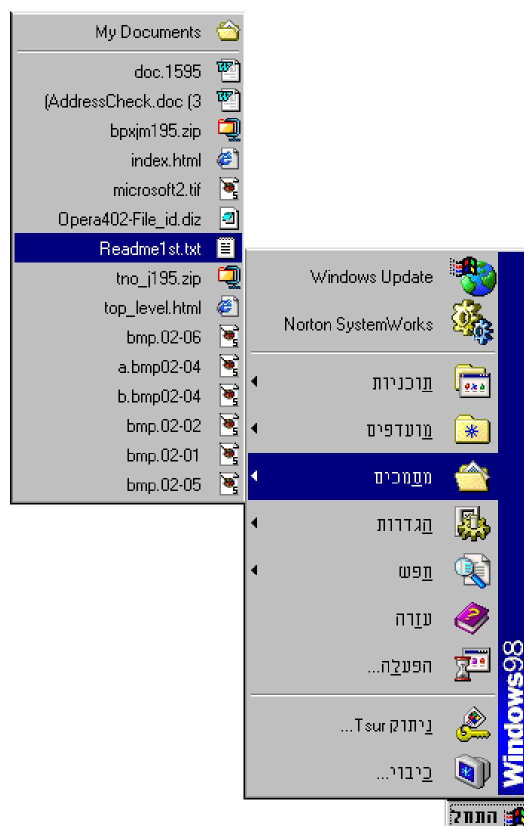


כדי לבדוק אם מישהו השתמש ביישום מסוים לפתיחת קבציך, בדוק את תפריט **קובץ** של היישום. בתחתית התפריט תמצא רשימת קבצים ממוספרת; אלה הקבצים שנפתחו לאחרונה באמצעות יישום זה. אם מופיע שם קובץ שלא פתחת לאחרונה, או סדר הקבצים שונה מאז שעבדת עם היישום, מישהו פתח את הקובץ/קבצים האמורים. במקרה זה, בדוק את מאפייני הקובץ/קבצים למידע נוסף (שים לב שרשימת הקבצים לא תהיה זמינה אם ביטלת אותה כמפורט בפרק 4).



הקפד לעיין במאפייני קובץ חשוד **לפני** פתיחתו. אם לא, יימחק מידע על הגישה האחרונה לקובץ זה כיון שאתה פתחת אותו בעצמך. Windows משנה מידע זה מייד עם פתיחת הקובץ.

דרך נוספת לבדיקת גישה לא מוסמכת לקובץ היא עיון בתפריט **מסמכים**, שבתפריט **התחל**. בחר **מסמכים** ותוצג הרשימה כמתואר בתרשים 2.5.



תרשים 2.5 תפריט **מסמכים** מציג את הקבצים שנפתחו לאחרונה על ידי כל היישומים במערכת.

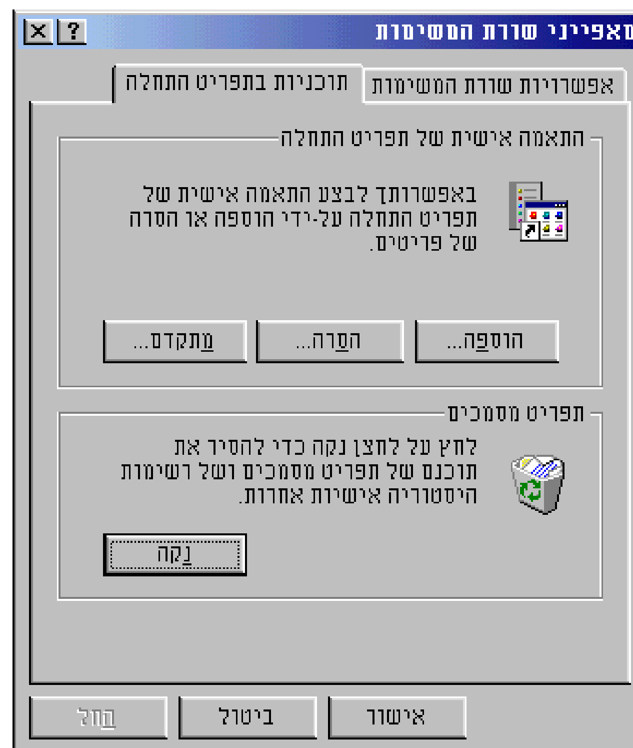
אם תראה שם קובץ שלא עבדת עליו לאחרונה, עיין במאפייני קובץ זה. אם שם הקובץ אינו מוכר לך לחלוטין, ייתכן שנוצר על ידי מישהו שהשתמש במחשב שלך; תיבת דו-שיח **מאפיינים** של הקובץ תציג את התאריך והזמן בו נוצר הקובץ.

לעיון באחד מקבצים אלה, פשוט לחץ על שמו; Windows תפתח אותו באמצעות היישום שיצר אותו.

מחיקת עקבותיך מתפריט המסמכים

ניתן להעלים עקבות מתפריט **מסמכים** בקלות!

1. בתפריט **התחל** לחץ על **הגדרות**, ובחר **שורת משימות**. תיבת הדו-שיח **מאפייני שורת המשימות** תוצג, כמתואר בתרשים 2.6.
2. לחץ על כרטיסיה **תוכניות בתפריט התחלה** בתיבת הדו-שיח של **מאפייני שורת המשימות**, ולחץ על הלחצן **נקה** תחת תפריט **מסמכים**.



תרשים 2.6 בעזרת תיבת הדו-שיח **מאפייני שורת המשימות**, תוכל למחוק את רשימת המסמכים מתפריט **מסמכים** בתפריט **התחל** של Windows

בעת כיבוי המחשב

אם בסביבתך נמצאים אנשים מיומנים בשימוש במחשבים, האפשרות היחידה היא לכבות את המערכת שלך. פעולה זו תרתיע חטטנים, כי אף אחד לא רוצה לגרום להשמעת צלילי האתחול ואותות אחרים המתרחשים בעת הדלקת מחשב, שיתריעו לבעלים שמישהו מדליק את המחשב שלו.



כדי לבדוק אם מישהו אתחל את המחשב וכיבה אותו בהיעדרך, ישנן מספר תוכנות שיסייעו לכך הנמצאות בתקליטור המצורף.

כיבוי מאובטח

אם בכוונתך להשאיר את המחשב ללא השגחה בלילה או לתקופה ארוכה, ודאי תרצה לכבותו. דבר זה עשוי להרתיע אנשים חסרי ידע במחשבים, כפי שהוזכר קודם.

לא תוכל, כמובן, לסמוך לחלוטין על הרתעה זו ברוב המקרים, כך שנדרשים אמצעים נוספים להגנה על המידע הרגיש שלך.

אמצעי זהירות בכיבוי

לפני כיבוי המחשב, עליך לבצע שתי פעולות להגנת המידע:

- לגבות קבצי נתונים חשובים
- להעתיק מידע רגיש לדיסקטים או מדיה אחרת ולאחסן את הדיסקטים במקום בטוח. כמו תמיד, מחק את קבצי הנתונים המקוריים.

מעבר לכך, שקול הסרת כבל כך שאיש לא יוכל להפעיל את המחשב. הבחירה הטובה ביותר היא כבל המתח למחשב עצמו (שים לב שאמצעי זה ניתן לביטול על ידי מישהו שיש לו כבל מתח - או יודע ויכול להעביר כבל ממחשב אחר).

ישנם אמצעי זהירות נוספים הכרוכים בשינוי הגדרות יישומים ו/או Windows. אלה נידונים בפרק הבא.

פרק 3



פשוט וישיר - הגנת המידע באמצעות סיסמאות והגדרות

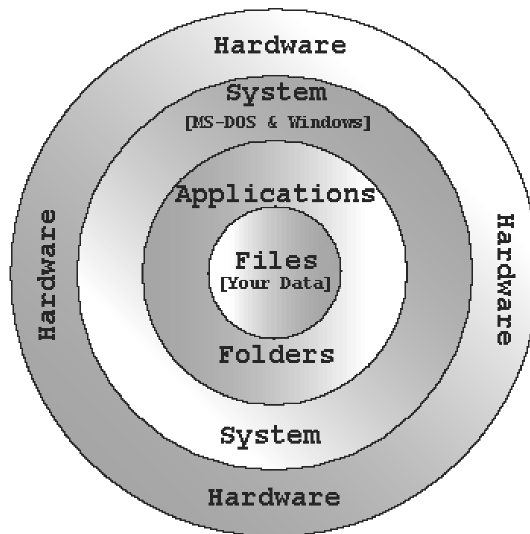
מה בפרק:

- *על מה להגן?*
- *הגדרות וכיוונים פשוטים שיגבירו את האבטחה*
- *הגנת הסיסמאות של Windows*
- *הגנה אמיתית באמצעות סיסמאות*

בפרק זה, נעיין בהגנת המערכת באמצעות סיסמאות של Windows, בנוסף לסיסמאות הגנה המסופקות על ידי תוכנות חיצוניות. נבחן גם כמה הגדרות וכיוונים פשוטים שניתן לעשות ב-Windows להגברה ניכרת של האבטחה.

על מה להגן: סקירה כללית

ניתן להסתכל על המחשב בשכבות, כאשר החומרה היא השכבה החיצונית, כמתואר בתרשים 3.1.



תרשים 3.1 "שכבות" המחשב.

השכבה הבאה היא Windows, ואחריה היישומים ומערכת הספריות (התיקיות) ולבסוף, הקבצים ותכולתם. כמובן, שברצונך להגן על המידע , אך אינך צריך לרכז את כל מאמציך במידע. כל שכבה יכולה להוות מוקד אבטחה. לפני שניכנס לפרטים על סיסמאות הגנה, להלן מספר דברים שעליך לדעת:

- **המחשב שלך ו-Windows -** כפי שנאמר לעיל, חומרת המחשב היא השכבה החיצונית. ההגנה מתחילה כאן בכך שתכבה את המערכת בהעדרך; אולם, לא תמיד זו הרתעה יעילה. חסימת גישה פיסית למערכת על ידי הצבתה במקום שאינו נגיש לכל אחד, כגון חדר נעול, היא השלב הבא. תוכל גם להסיר רכיבים פיסיים כגון כבל החשמל וכבל המקלדת. כמובן, אמצעים אלה אינם תמיד מעשיים - במיוחד במקום העבודה או בעת שימוש במחשב של מישהו אחר.

  Windows כשלעצמה מציעה מספר מערכות סיסמה, אך רק לאחת יש ערך מעשי, וכפי שנלמד, ניתן לעקפה בקלות.

- **יישומים -** ניתן להגן על יישומים במספר צורות. תוכל לשנות את שמות היישומים כך שייראו כמו משחקים או קבצים שאין להם קשר ליישום. כמו כן ניתן להסתיר יישומים במספר דרכים שונות - כגון הכנסתם לתיקיות "לא נכונות", או שימוש בשמות מטעים לתיקיות או קבצים, כפי שיפורט בפרק 4.

- **תיקיות -** ניתן להסתיר או לשנות את שמות התיקיות שעל הדיסק הקשיח או הדיסקט. בעזרת תוכנה מתאימה, ניתן להוסיף סיסמת הגנה לתיקיות (Windows גם מספקת הגנה באמצעות סיסמאות לתיקיות ותכולתם עבור רשתות **בלבד**). או שתוכל להשתמש בטכניקות אחרות למנוע מחטטנים המדפדפים לפי תיקיות לגשת לקבצים החשובים ביותר.
- **קבצים -** מספר יישומים מספקים סיסמאות הגנה לקבציהם. Windows מאפשרת הגנה באמצעות סיסמה על קבצים מסוימים במערכות מרושתות כך שלא ניתן לשתף קבצים אלה ברשת. כמו בשמות תיקיות ויישומים, תוכל לשנות שם של קובץ או להסתירו. ניתן גם להשתמש במספר תוכנות סיסמה כלליות להגנת קבצים, שבהם נדון בקרוב בפרק זה.

אבטחה באמצעות הגדרות וכיוונים פשוטים

ישנן מספר הגדרות וכיוונים שתוכל לעשות בעצמך, המחזקים את אבטחת Windows. חלק מהם הוצגו בפרק 2, וכאן נדון בהם ביתר פירוט. כל האמצעים הנידונים הם חינם, קלים להפעלה, וכוללים :

- מחיקת תוכן תפריט מסמכים מעת לעת.
- ריקון סל המיחזור, או שינוי הגדרותיו.
- הסרה או שינוי שמות סמלי קיצורי הדרך בשולחן העבודה.
- הסרה או שינוי שמות תוכנות בתפריט **התחלה**.
- הסתרת סרגל המשימות.
- מניעת שינוי או מחיקת קובץ.
- מניעת שינוי או מחיקת תיקיה.

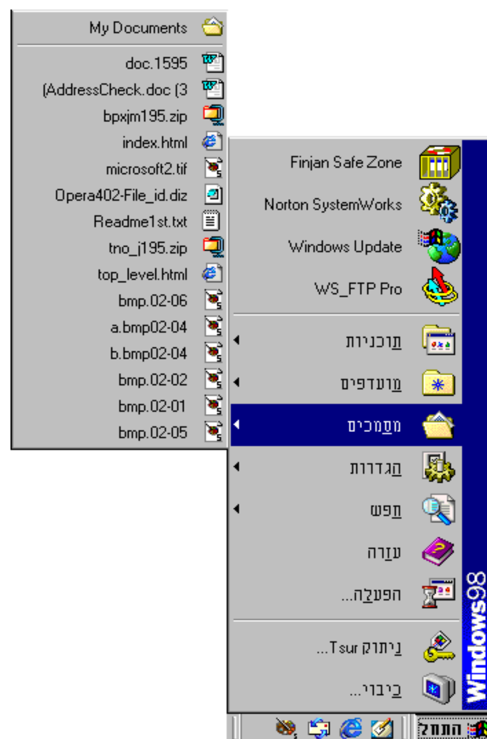
מחיקת תוכן תפריט המסמכים

המקום הראשון להסרת עקבותיך הוא תפריט **מסמכים** בתפריט **התחלה** של Windows. דנו בו בפרק 2, וכעת נדון בו ביתר פירוט. הצג את תפריט **התחלה** ובחר **מסמכים**. תוצג רשימה של כ- 15 קבצים אחרונים שפתחת באמצעות יישום כלשהו, כמתואר בתרשים 3.2.

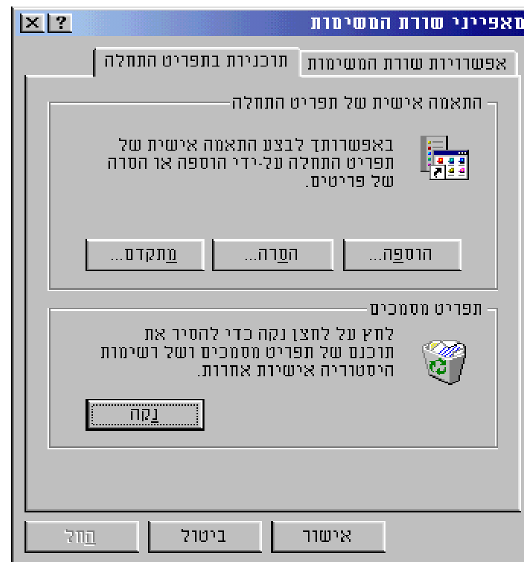
לחיצה על אחד משמות הקבצים האלה מפעילה את היישום, ופותחת את הקובץ. המשמעות היא שכל אחד יכול לעיין בקבצים עליהם עבדת לאחרונה בלי אפילו לטרוח לחפש.

למזלך, קל ופשוט למחוק תפריט זה. לחץ על תפריט **הגדרות**, ובחר את **סרגל המשימות**. לחץ על כרטיסיה **יישומי תפריט התחלה**, ולחץ על לחצן **נקה** שבתחתית הכרטיסיה, כמתואר בתרשים 3.3 (שים לב **שאינך** מוחק קבצים בדרך זו. רק רשימת שמות הקבצים נעלמת).

ברגע שהתפריט ריק, חטטנים יאלצו לטרוח מעט יותר כדי למצוא את קבציך. אם התמזל מזלך, הם פשוט יתייאשו ויעזבו.



תרשים 3.2 תפריט **מסמכים** של Windows.



תרשים 3.3 מחיקת התכולה של תפריט **מסמכים**.

ריקון והגדרת סל המיחזור

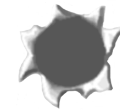
סל המיחזור הוא פירצה שבה חטטנים יכולים "לדוג" מידע. כמצוין בפרק 2, סל המיחזור שומר כל קובץ שמחקת באמצעות סייר Windows או יישום Windows אחר כמו Word. כך, כל אחד יכול לבחון קבצים שמחקת.

ישנן שלוש דרכים לטפל בבעיה זו:

❖ רוקן את סל המיחזור מדי יום או לעיתים תכופות יותר. עשה זאת על ידי לחיצה ימנית על סל המיחזור ובחירת **רוקן סל מיחזור**, או לחיצה כפולה על סל המיחזור ובחירת **קובץ** ולחיצה על **רוקן סל מיחזור**.

❖ הגדר את סל המיחזור כך שקבצים יימחקו לצמיתות (נגענו בשיטה זו בפרק 2, אך כאן ניכנס לפרטים). כדי לעשות כן, פתח את סל המיחזור, בחר **מאפיינים** מתפריט **קובץ**, לחץ על הכרטיסיה **כללי**, ולחץ על לחצן האפשרויות **אל תעביר קבצים לסל המיחזור, הסר קבצים מייד עם מחיקתם**, לסיום לחץ **אישור** (לא תוכל לשחזר קבצים לאחר הגדרה זו).

❖ מחק קבצים דרך DOS. מתפריט **התחלה**, בחר **תוכניות**, ועבור **להפניה ל-MS-DOS**; ב-DOS עבור לתיקיה המכילה את הקבצים שברצונך למחוק; הקלד **DEL**, ולאחריו את שם הקובץ שברצונך למחוק.



לא קל לשחזר קבצים שנמחקו דרך DOS - אם בכלל ניתן לשחזרם. בנוסף, קל מאוד למחוק את הקובץ הלא נכון ב-DOS. אי לכך, מומלץ לא להשתמש בפקודת DEL של DOS אלא אם אתה רגיל לעבוד ב-DOS (בדומה, אם תגדיר את סל המיחזור כך שלא יעביר קבצים, לא תוכל לאחזר אותם).

פתרון יצירתי

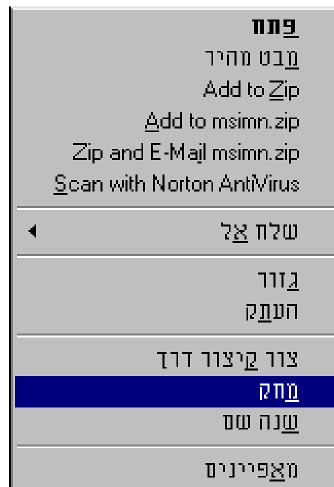
אם נתקלת בחטטן מתוחכם יותר, וברצונך להשלותו שאינך מוחק קבצים מסל המיחזור, ועקב כך אין לך מה להסתיר, נסה למחוק רק את קבציך הרגישים באופן סלקטיבי מסל המיחזור.

הסיבה לכך היא, שאם מישהו יבחין שמחקת את כל הקבצים מסל המיחזור, זה עשוי לעודד אותו להמשיך ולחפש. כך, כשהוא רואה קבצים בסל המיחזור הוא מתרכז בהם, בעוד את מה שבאמת רצית להסתיר כבר מחקת מזמן.

הסרה ושינוי שמות קיצורי דרך משולחן העבודה

בהינתן להם גישה, אנשים רבים יתחילו ללחוץ ולהפעיל סמלי קיצור דרך רק כדי לראות מה הם ומה הם מפעילים. תוכל למנוע זאת על ידי מחיקת סמלי קיצור הדרך או שינוי שמם. אם תשנה שם של קיצור דרך לשם מטעה ולא מעניין (כגון **כלי מערכת**), ייתכן שיתעלמו ממנו. שינוי שם היא חלופה רק אם אתה חייב שקיצור הדרך יהיה על שולחן העבודה (שוב, ודא **שאתה** זוכר איך קראת לו).

- למחיקת סמל על שולחן העבודה, לחץ עליו לחיצה ימנית, ובחר **מחק** מהתפריט, כמתואר בתרשים 3.4.
- לשינוי שמו של קיצור דרך, לחץ עליו לחיצה ימנית, ובחר **שנה שם** בתפריט. עתה תוכל להקליד שם חדש לקיצור דרך זה.



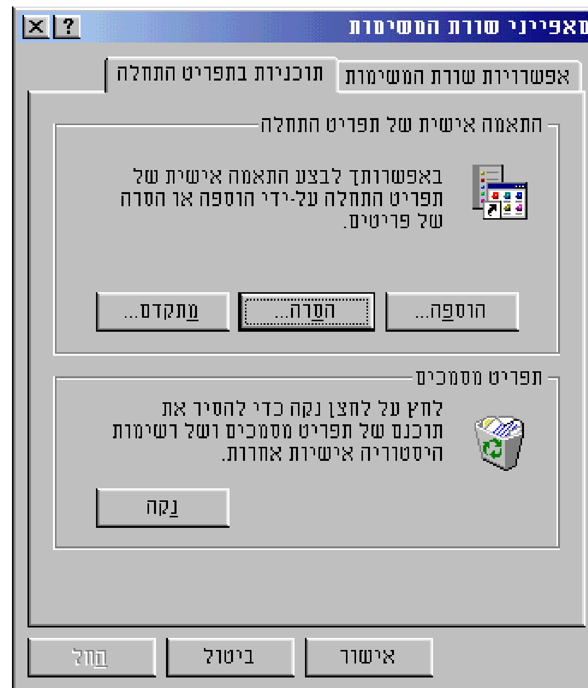
תרשים 3.4 מחיקת סמל משולחן העבודה

הסרה ושינוי פריטים בתפריט התחלה

ניתן לשנות שם ולמחוק פריטים בתפריט **התחלה** בקלות, ובכך למנוע חיטוט בדיסק הקשיח ביעילות.

מחיקת פריט מתפריט התחלה

למחיקה או שינוי פריטים בתפריט **התחלה**, לחץ לחיצה ימנית על **שורת המשימות** ובחר **מאפיינים** (Properties), או בחר **הגדרות** ולחץ על **שורת משימות**, מתפריט **התחלה**. לחץ על כרטיסיית **יישומי תפריטי התחלה**, להצגת תיבת דו-שיח כמתואר בתרשים 3.5.

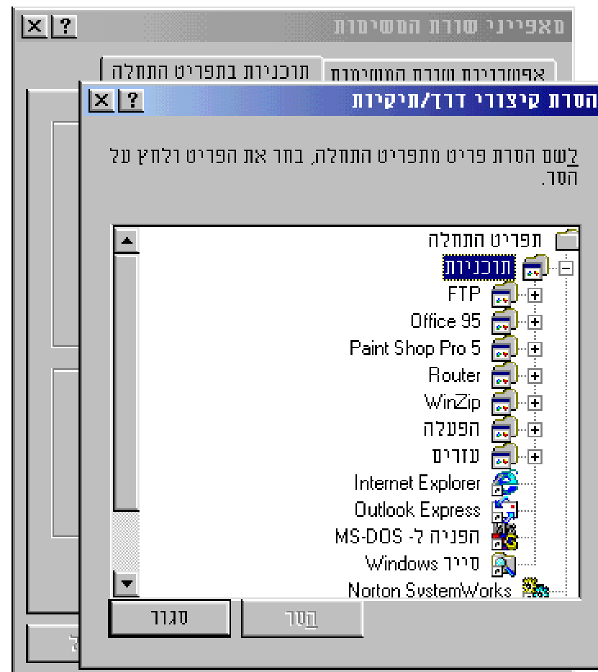


תרשים 3.5 תיבת הדו-שיח של מאפייני שורת המשימות, כאשר כרטיסיית **תוכניות בתפריט התחלה** מוצגת

להסרת פריט מתפריט **התחלה**, לחץ על לחצן **הסרה** בתיבת הדו-שיח של **מאפייני שורת המשימות**. יוצג חלון המכיל רשימת תיקיות בדיסק הקשיח, כמתואר בתרשים 3.6. ניתן למחוק תיקיות אלו, לדפדף בהן, או למחוק קבצי תוכנה. לביצוע מחיקה, שזה עיקר עניננו כאן, לחץ על הפריט הרצוי, ולחץ על לחצן **הסר**.

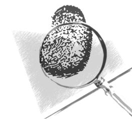
הפריטים שהסרת מתפריט **התחלה** יישארו על הדיסק הקשיח, כך שתוכל עדיין להשתמש בהם. עדיין תוכל להריץ תוכנה שהוסרה מתפריט **התחלה** באמצעות פקודת **הפעלה** בתפריט **התחלה**, או באמצעות קיצור דרך בשולחן העבודה. כמו כן תוכל עדיין לגשת לתיקיות וקבצים שהוסרו מתפריט **התחלה** באמצעים הרגילים.

- להרצת תוכנית שאינה בתפריט **התחלה**, פתח את תפריט **התחלה** ולחץ **הפעלה** (Run). הכנס את שם התוכנית בתיבת הדו-שיח של **הפעלה** ולחץ **אישור**.
- להרצת תוכנית עם קיצור דרך על שולחן העבודה, לחץ פעמיים על סמל התוכנית בשולחן העבודה. אם אין קיצור דרך, תוכל ליצור אותו. לחץ לחיצה ימנית על שולחן העבודה, לחץ **חדש**, ולחץ **קיצור דרך**. עקוב אחר ההוראות בתיבת הדו-שיח **יצירת קיצור דרך** (בעיקרון, הכנס את שם ומיקום התוכנית שברצונך להריץ, ושם לקיצור הדרך).



תרשים 3.6 תיבת הדו-שיח הסרת קיצורי דרך/תיקיות

דרך נוספת להרצת תוכנות היא להתחיל בסמל **המחשב שלי** או להשתמש בסייר Windows כדי לנווט דרך התיקיות ותת התיקיות עד לתוכנה עצמה. לאחר שהגעת לתוכנה שברצונך להפעיל, לחץ עליה פעמיים להרצתה.

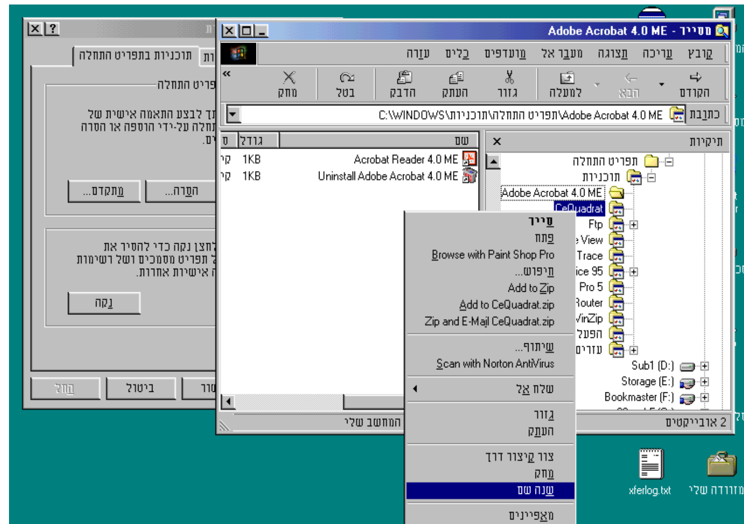


זכור, פריטים שנמחקו מתפריט **התחלה** אינם נמחקים מהדיסק הקשיח.

עריכה/שינוי שם של פריטים בתפריט התחלה

לשינוי שם פריט בתפריט **התחלה**, לחץ על לחצן **מתקדם** המופיע בכרטיסיה **אפשרויות שורת המשימות** של תיבת הדו-שיח **מאפייני שורת משימות** המתוארת בתרשים 3.5. **סייר Windows** ייפתח ויציג את תיקיית **תפריט התחלה**. לשינוי שם פריט, לחץ עליו לחיצה ימנית ובחר **שינוי שם** מהתפריט המופיע, כמתואר בתרשים 3.7.

הקלד את השם החדש בתיבת הדו-שיח המופיעה (תוכל גם למחוק פריטים מתצוגה זו, על ידי בחירת **מחק** במקום **שנה שם** מהתפריט).



תרשים 3.7 סייר Windows ובו תיקיית תפריט התחלה

הסתרת שורת המשימות

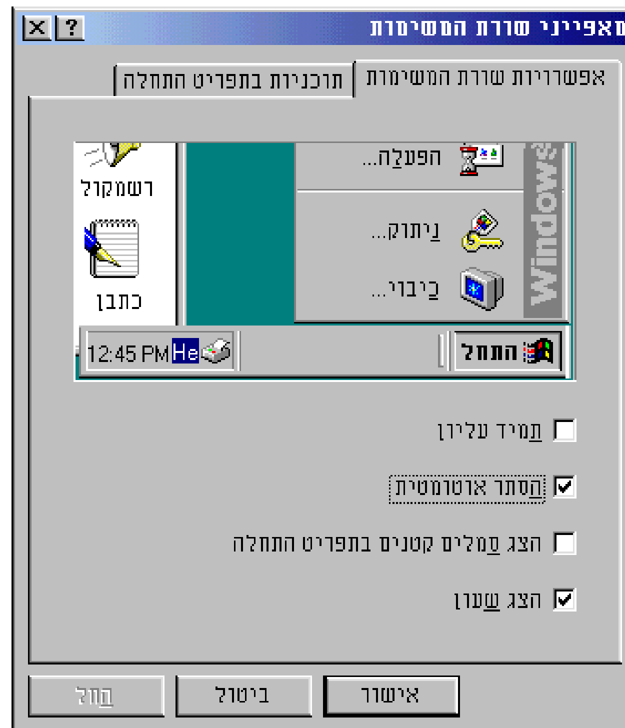
הגדרה פשוטה של **שורת משימות** שתרתיעי חטטן אל מתוחכם וסקרנים מזדמנים היא **הסתר אוטומטית.** כמתואר בתרשים 3.8, בחירה זו מסתירה למעשה את שורת המשימות, ומסתירה את תפריט **התחלה** ותוכנות נוכחיות שרצות (מה שבעצם קורה, זה ש**שורת המשימות** "נדחפת" אל מחוץ לאזור הצפייה הרגיל, אף שהיא תוצג אם סמן העכבר יונח מעל מיקומה בקצה המסך.

להגדרת מאפיין זה, עקוב אחר השלבים שלהלן:

1. לחץ **התחל**.
2. לחץ **הגדרות** ובחר את **שורת משימות** כדי לפתוח את תיבת הדו-שיח **מאפייני שורת המשימות**.
3. לחץ על כרטיסיה **אפשרויות שורת המשימות,** אם נדרש.
4. סמן את תיבת הסימון **הסתר אוטומטית**, ולחץ **אישור**.



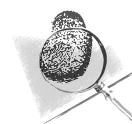
זה קל מאוד להפעלה. לחיצה על Ctrl+Esc ו...שורת המשימות מופיעה במלוא הדרה.



תרשים 3.8 הגדרת אפשרות שורת המשימות

מניעת שינוי קובץ

כאשר יש חשש שמישהו ישנה בטעות (או בכוונה) את קבציך, Windows מספקת הגנה קטנה כנגד זה. ניתן להשתמש ב**סייר Windows** להגדרת מאפיינים מתאימים כך שלא ניתן יהיה לשנות קבצים, על ידי הגדרת אפשרות **קריאה-בלבד**.

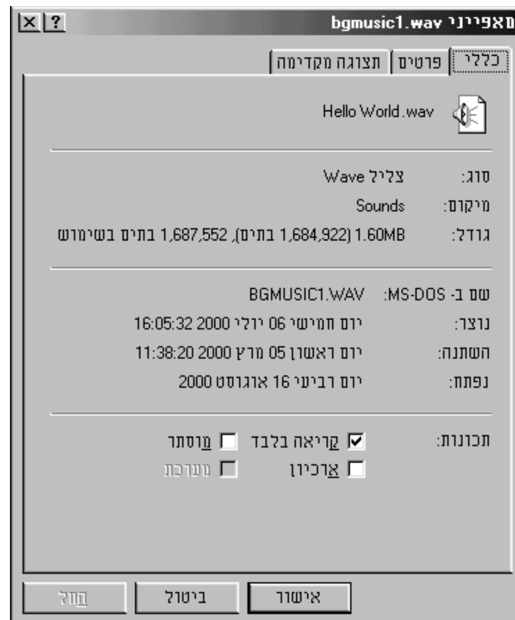


מאפיין **קריאה-בלבד** הוא הגדרת מערכת הפעלה המונעת שינויים בקובץ. ניתן לעיין או להעתיק קובץ, אך לא ניתן לשנות את שמו או תכולתו - ומכאן השם **קריאה-בלבד**. אבל, ניתן לעיין בו ולשמור אותו בשם אחר ולכן זאת הגנה מאוד מאוד מינימלית.

עקוב אחר השלבים הבאים להגדרת אפשרות זו:

1. הפעל את **סייר Windows**.
2. פתח את התיקיה המתאימה, ולחץ לחיצה ימנית על הקובץ שברצונך להגן. עתה בחר **מאפיינים** מהתפריט המוצג. תופיע תיבת דו-שיח **מאפיינים** כמתואר בתרשים 3.9.

3. סמן את תיבת הסימון **קריאה-בלבד** ולחץ על לחצן **אישור**. הקובץ מוגן עתה מעריכת שינויים.

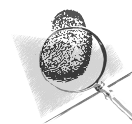


תרשים 3.9 תיבת הדו-שיח **מאפייני קובץ** עבור קובץ בשם bgmusic1.wav



אם ברצונך לשנות מספר קבצים באותה תיקיה לסטטוס **קריאה-בלבד**, בחר את כל הקבצים. היעזר במקשים Ctrl ו- Shift. עתה לחץ לחיצה ימנית על שם קובץ כלשהו להצגת תיבת הדו-שיח **מאפייניים** והגדרת מאפיין **קריאה-בלבד** עבור כל הקבצים הנבחרים בבת-אחת.

המאפיין **קריאה-בלבד** מונע עריכה ושמירת קובץ באמצעות יישום DOS או Windows. המאפיין גם מונע מחיקה מ-DOS. אולם, עדיין ניתן למחוק את הקובץ ל**קריאה-בלבד** באמצעות **סייר Windows**, אף שהסייר ישאל קודם אם אכן ברצונך למחוק את הקובץ. אך כיון שלא בהכרח אתה תהיה האדם שיישאל שאלה זו, הייה מודע שזו אינה שיטה בטוחה לחלוטין מחבלה בזדון.

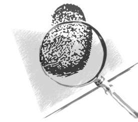


ניתן להגדיר קבצים הנוצרים ביישומים מסוימים, כגון Word, ל**קריאה-בלבד** בעת שמירתם. יישומים מסוימים מאפשרים יצירת הגדרה זו, או שתוכל להשתמש בתיבת הדו-שיח **מאפייניים** של הקובץ, הניתנת לפתיחה באמצעות **סייר Windows**. ניתן גם להגן על קבצים באמצעות סיסמאות ברבים מיישומים אלה. נושא סיסמאות יידון ביתר פירוט בפרקים 4 ו- 5.

מניעת שינוי ומחיקת תיקיה

ניתן להגן על תיקיות שלמות משינוי שם ומחיקה בצורה זהה לקבצים בודדים כדלקמן:

1. התחל את **סייר Windows**.
2. סמן את התיקיה/תיקיות שברצונך להגן.
3. לחץ לחיצה ימנית, ובחר **מאפיינים** בתפריט שיוצג.
4. לחץ על לחצן האפשרויות **קריאה-בלבד** ולחץ **אישור**.



ניתן להגדיר את המאפיין **מוסתר** (Hidden Attribute) (אשר לחצן האפשרויות שלו מופיע בדף **כללי** של תיבת הדו-שיח **מאפיינים**), כך שיסתיר קבצים מיישומי Windows ו-DOS. המאפיין **מוסתר** הוא הגדרת מערכת הפעלה, שכשמה, מסתירה קובץ או תיקיה מרשימות תכולה של תיקיות ויישומים. עוד נדון בכך בהמשך בפרק 5.

מערכת הסיסמאות של Windows

מערכת הסיסמאות של Windows 95/98/ME אינה יעילה במיוחד למטרות אבטחה, כיון שהיא תוכננה יותר לשמור על העדפות משתמשים רבים מאשר כמערכת הגנה. בכל זאת, ישנם כמה רכיבים המספקים מידה של הגנה, כגון סיסמת שומר-מסך והגנת רשת לקבצים ותיקיות. כמוזכר, מערכת-סיסמאות-משתמשים אינה יעילה במיוחד במונחים של הגנה על קבצים, אך מערכת הגנת התחברות-חיוג מוגנת-סיסמה, כן יעילה להגנה.

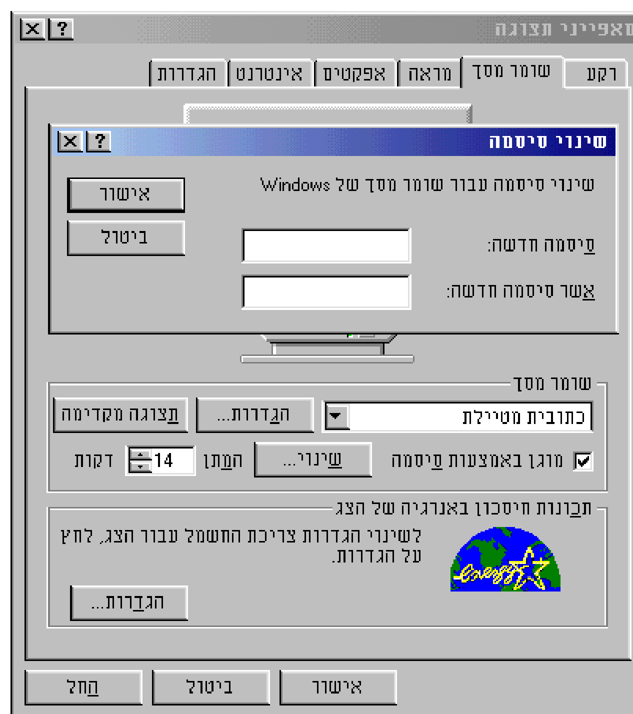
ישנה גם מערכת סיסמת אתחול הניתנת לגישה באמצעות **הגדרות** CMOS) CMOS הוא קיצור של Complementary Metal Oxide Semiconductor). ב-CMOS מאוחסנות הגדרות רכיבי החומרה במחשב. אלו כוללות את התאריך והשעה, נתונים על סוגי הדיסקים הקשיחים, ועוד. המידע מאוחסן בשבב - מסוג CMOS - שיש לו זיכרון ניתן-לתכנות הפועל באמצעות סוללה זעירה. המחשב קורא מידע זה בכל הפעלה. אנו נבחן אמצעים אלה בעמודים הבאים.

סיסמאות של שומרי מסך

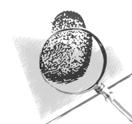
מערכת סיסמאות שומר מסך היא מערכת הגנה ראשונית בה תוכל להשתמש כאשר עליך להעדר מהמחשב לזמן קצר, אך אינך רוצה לכבותו. בעת הגדרה של סיסמת שומר-מסך, המערכת תדרוש סיסמה **לאחר** ששומר המסך הופעל. להגדרת סיסמת שומר מסך עקוב אחר השלבים הבאים:

1. מתפריט **התחלה** בחר **הגדרות**, ובחר **לוח בקרה**. לחץ לחיצה כפולה על **תצוגה** (לחליפין ניתן ללחוץ לחיצה ימנית בשולחן העבודה ולבחור **מאפיינים**). תיבת הדו-שיח **מאפייני תצוגה** תופיע.
2. לחץ על כרטיסיה **שומר מסך** ולחץ על לחצן האפשרויות **מוגן באמצעות סיסמה**. עתה לחץ על לחצן **שינוי** שלידה, והכנס סיסמה בתיבת הדו-שיח המתקבלת, כמתוארת בתרשים 3.10 (עליך להכניס את הסיסמה פעמיים כדי לאשר אותה).

מערכת ההגנה של סיסמת שומר מסך יעילה אם אתה מתכוון להיעדר מהמחשב לזמן קצר. אך עליך להיות מודע לחולשה גדולה במערכת: אם מישהו באמת רוצה לחדור למחשב שלך, כל שעליו לעשות הוא לכבות את המחשב ולחזור ולהדליקו. אין הגנת סיסמה עד ששומר המסך לא יופעל מחדש.



תרשים 3.10 תיבת דו-שיח **מאפייני תצוגה** והכרטיסיה של תיבת דו-שיח **שינוי סיסמה**



למשתמשי Windows NT יש אפשרות נוספת בכל הנוגע לסיסמאות הגנה: נעילת תחנת העבודה, באמצעות שומר המסך. כאשר תחנת העבודה נעולה, איש לא יוכל לחדור למערכת ללא סיסמת המשתמש הנוכחי. ויש עוד; כל מי שינסה לאתחל את המערכת כדי לעקוף את הגנת הסיסמה, עדיין יצטרך להשתמש בסיסמת המשתמש האמור כדי להיכנס למחשב. כמובן שכל אדם עם זכויות ניהול עדיין יוכל להתחבר, ובכך לדרוס את הגנת הסיסמה.

הגנת סיסמה חזקה יותר באמצעות שומר המסך

אם ברצונך ליצור הגנת אתחול עם שומר המסך, פעל כדלקמן: הגדר סיסמה בכרטיסיה **שומר המסך** שבתיבת הדו-שיח **מאפייני תצוגה**. בעזרת **סייר Windows**, אתר קובץ עם סיומת SCR., השייך לשומר המסך הפעיל שלך (קבצים בעלי סיומת SCR. נמצאים בתיקיית windows/system/ ויש להם שמות המתאימים לשומרי המסך ברשימה שבתיבת הדו-שיח של מאפייני התצוגה).

לחץ לחיצה ימנית על קובץ שומר המסך וגרור אותו לתיקיה הבאה:

/Windows/Start Menu/Programs/StartUp

יופיע תפריט. בחר **צור קיצור דרך**. עתה שומר המסך שהגדרת יופעל כאשר Windows יופעל ויבקש סיסמה.

פרופילים וסיסמאות עבור משתמשים רבים

Windows מציעה אפשרות של פרופיל אישי כאשר יש משתמשים רבים, הוא שומר פרמטרים של העדפות אישיות כגון מבנה שולחן העבודה, צורתו, פריטי תפריט **התחלה** וכן הלאה.

ההגדרות לכל משתמש מוגנות על ידי סיסמה, אך זו אינה חוסמת גישה ליישומים או לתוכנות כלשהן. כאשר מאותחל מחשב שבו הגדרות אישיות שונות למשתמשים רבים, תיבת דו-שיח תדרוש שם משתמש וסיסמה. אולם, ניתן לעקוף זאת על ידי לחיצה על Esc או לחיצה על לחצן **ביטול**.

אם ברצונך להגדיר פרופילים למספר משתמשים, לחץ על תפריט **התחלה** בחר את **הגדרות** ולחץ על **לוח בקרה.** לחץ לחיצה כפולה על סמל **סיסמאות**. תופיע תיבת דו-שיח **מאפייני סיסמאות**, המסבירה את עצמה. אולם, שוב, הגדרות שתבצע כאן אינן קשורות לאבטחת הקבצים, תוכנות, או מערכת ההפעלה שלך.

סיסמאות חיוג

מערכת סיסמאות החיוג של Windows דורשת שם משתמש וסיסמה, המשמשים להתחברות למערכת מקוונת שאליה מתבצע החיוג. אולם, שים לב, שגם הגדרת סיסמה זו חסרת משמעות במונחים של אבטחת מערכת. הסיסמה ושם המשתמש משמשים להתחברות למערכת מקוונת כגון ISP (ספק שירות אינטרנט). כמתואר בתרשים 3.11, יש לחצן אפשרויות בשם **שמור סיסמה** בתיבת הדו-שיח **התקשרות אל**.

הסיסמה נשמרת, אך רק במהלך ההפעלה הנוכחית; הסיסמה מתבטלת עם כיבוי המחשב (הסיבה העיקרית לנוכחות סיסמה כאן, היא לפשט התחברויות חוזרות למערכת מקוונת). אי סימון תיבת הסימון **שמור סיסמה** ימנע ממישהו להתחבר למערכת עם זיהוי המשתמש (User ID) והסיסמה שלך, אך זהו כל גבול האבטחה כאן.

התקשרות אל

ספק שירותי אינטרנט

שם המשתמש: theduck

סיסמה: *********

שמור סיסמה

מספר טלפון: 7654321

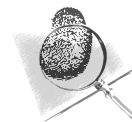
מתחייג מ: מיקום חדש

מאפייני חיוג...

צור קשר

ביטול

תרשים 3.11 תיבת הדו-שיח **התקשרות אל** עם אפשרות **שמור סיסמה**.

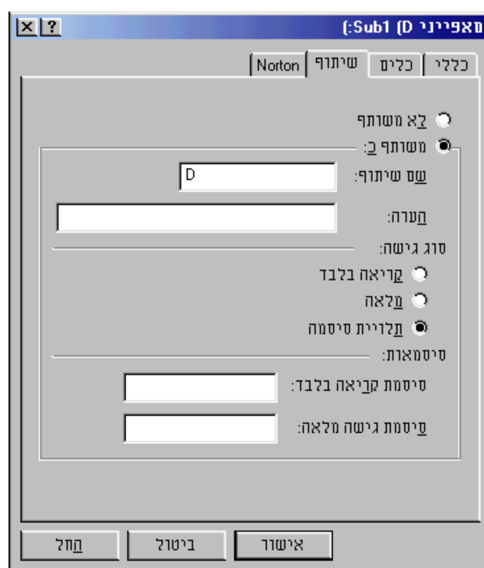


אם המחשב שלך מוגדר לאחד או יותר משתמשים, סביר להניח שבעת הפעלת המחשב תראה תיבת דו-שיח המבקשת ממך שם וסיסמה. אם תדלג על תיבת דו-שיח זו (על ידי לחיצת **ביטול** או **Esc**), לחצן האפשרויות **שמור סיסמה** לא יהיה זמין בתיבת הדו-שיח **התקשרות אל**. אם התחברת, כנדרש, עם זיהוי משתמש (ID) וסיסמה, עשה שימוש בסיסמה זו גם בתיבת הדו-שיח **התקשרות אל**.

הגנת קבצים ותיקיות ברשת באמצעות סיסמאות

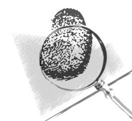
אם אתה משתמש במחשב המחובר ברשת במקום העבודה, תוכל להקצות גישה ולהגן על קבצים ו/או תיקיות על ידי הגדרת מאפייני קבצים או תיקיות.

הדרך המהירה ביותר להגיע למאפייני קובץ או תיקיה היא להתחיל את **סייר Windows**, וללחוץ לחיצה ימנית על הקובץ או התיקיה הנדרשים. בחר **מאפיינים** מהתפריט. תופיע תיבת דו-שיח **מאפיינים**, כמתוארת בתרשים 3.12.



תרשים 3.12 מאפיינים בכרטיסיית השיתוף של תיקיה.

במערכת מרושתת, לתיבת הדו-שיח **מאפיינים** של תיקיה יש שתי כרטיסיות: **כללי** ו**שיתוף**, ולתיבת הדו-שיח **מאפיינים** של כונן מצטרפת גם הכרטיסיה **כלים** (ראה תרשים 3.12). תוכנות מסוימות מוסיפות בעת התקנתן כרטיסיות נוספות לתיבת דו-שיח זו (ראה בתרשים 3.12 את הכרטיסיה **Norton**). אם ברצונך לאפשר גישה לקובץ או תיקיה רק באמצעות סיסמה, לחץ על כרטיסיה **שיתוף**. כרטיסיית **שיתוף** תופיע ובה תוכל לבצע בחירות לגבי סוג הגישה. אם ברצונך להגדיר את סוג הגישה (**קריאה-בלבד**, או **מלאה** או **תלויית סיסמה**) לקובץ או תיקיה, גש לכרטיסיה **כללי**, המפורטת בהמשך ספר זה.



מנהל הרשת יכול, כמובן, לגשת לכל קובץ, תיקיה ותוכנה במערכת שלך, בין אם הם מוסתרים או מוגנים על ידי סיסמה ובין אם לאו.

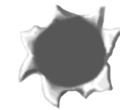
סיסמאות אתחול ברמת ה-CMOS

מערכת סיסמאות אתחול דורשת הכנסת סיסמה מייד עם הפעלת המחשב. לאחר שהותקנה, המחשב לא יטען את מערכת ההפעלה עד להכנסת הסיסמה הנכונה.

ההליך המדויק להגדרת סיסמת אתחול שונה ממחשב למחשב - לעיתים יש אף הבדלים בין מחשבים של אותו יצרן. אולם, השלב הראשון בהגדרת סיסמת אתחול היא לגשת להגדרות CMOS של מערכת ההפעלה. דבר זה מתבצע לרוב על ידי הקשת F1 או מקש ייעודי אחר בעת האתחול (הודעה על איזה מקש ללחוץ תופיע עם הפעלת המחשב). משם, עקוב אחר ההוראות וההנחייה על המסך להגדרת הסיסמה.



סיסמת האתחול ניתנת לעקיפה על ידי מישהו שמאתחל את המחשב באמצעות דיסקט מערכת הפעלה מכונן A. כדי למנוע זאת, היכנס להגדרות CMOS, ואתר הגדרה בשם Boot Options (אפשרויות אתחול). בחר אפשרות זו. עקוב אחר ההנחיות עד שתגיע להגדרה enable/disable setting for Boot From Floppy, Check Drive A (אפשר/מנע אתחול מכונן A) או דומה לזה.



הקפד על זהירות יתרה כאשר אתה נכנס להגדרות CMOS של מערכת ההפעלה! ניתן בקלות לשתק את מערכת ההפעלה על ידי פעולה כמו הגדרה שגויה של סוג הדיסק הקשיח. עליך גם לדעת שהסרת סיסמת אתחול, אם שכחת אותה, היא משימה מתישה וקשה.

שיטת הגנה יעילה: תוכנת סיסמאות אמיתית

אף שסיסמאות הגנה לרשתות של Windows פועלות היטב לתקופה קצרה, ולסיסמת שומר המסך יש שימושים, תוכנת סיסמאות אמיתית היא הדרך היעילה היחידה להגיע לרמת אבטחה גבוהה עבור קבצים, תיקיות, או המערכת כולה. תוכל להחליף את הגנת הסיסמאות הגבולית של Windows בעזרת תוכנות שיתופיות (Shareware) ותוכנות מסחריות המספקות הגנה אמיתית. אנו נבחן כמה מהן כאן.

שים לב שהתוכנות הנידונות בעמודים הבאים הן מדגם של המוצרים הזמינים הטובים יותר. יש מוצרים אחרים המספקים תכונות זהות שלא נכללו כאן עקב מגבלות מקום.

לרוב התוכנות המוזכרות כאן יש תכונות נוספות מעבר לאספקת הגנה באמצעות סיסמאות. לכן, הן תופענה שנית בפרקים מאוחרים יותר וחלקן אף יהיו בתקליטור המצורף.

תוכנות שיתופיות (Shareware)

תוכנות שיתופיות הן שיטה טובה לנסות תוכנה לפני רכישתה, וככלל, מעודדים שיתוף עותקי תוכנות שיתופיות. ההנחה הבסיסית שמאחורי תוכנה שיתופית היא פשוטה: נסה את התוכנה, ואם היא לטעמך, שלם את דמי הרישום. אם התוכנה לא מוצאת חן בעיניך, אינך משלם. כל זאת נעשה על בסיס כבוד ואמון. אתה מקבל תוכנה שיתופית חינם על ידי הורדתה מהאינטרנט, או השגת העתק מחבר, או העתקה מדיסק או תקליטור, כגון התקליטור המצורף לספר זה.

חלק מהתוכנות השיתופיות מתפקדות באופן מלא. תוכנות שיתופיות אחרות מציעות תפקוד מוגבל בלבד, וחלקן פועלות רק לפרק זמן קבוע מראש. לרבות מהן יש תזכורות קופצות המעודדות את המשתמש לשלם דמי רישום. ההגבלות על תוכנה שיתופית לא רשומה מבוטלות, כאשר אתה משלם דמי רישום ומקבל קוד הפותח את נעילת התוכנה.

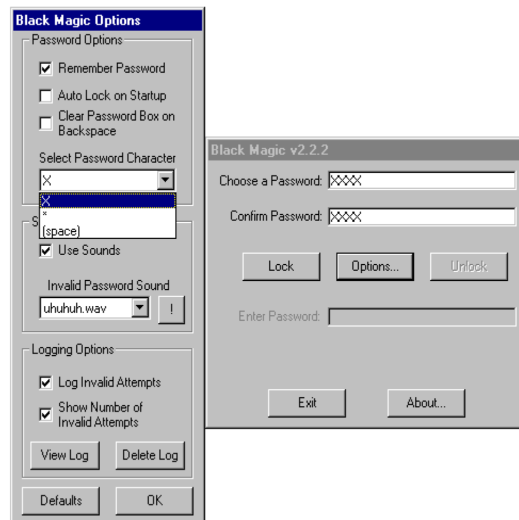


ניתן להוריד תוכנות שיתופיות מהכתובת www.tucows.co.il **וגם** מאתרי אינטרנט רבים אחרים כגון: Download.com, Shareware.com **ו-**Wugnet.com.

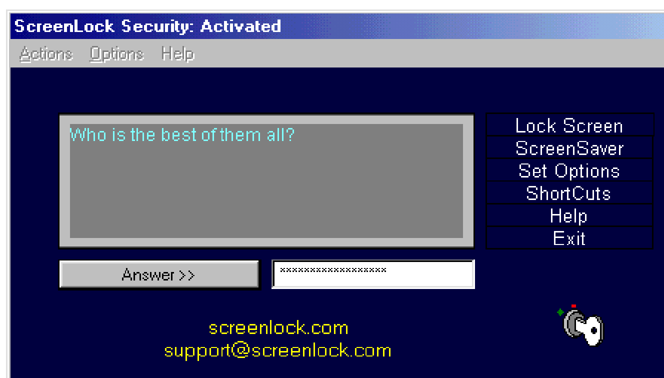
ישנן תוכנות שיתופיות, ותוכנות הגנה באמצעות סיסמאות עבור כמעט כל יישום, מעיבוד תמלילים ועד גיליונות אלקטרוניים. התוכנות השיתופיות הבאות מציעות סיסמאות הגנה איתנות, וזו הסיבה שהן מוזכרות כאן.

Black Magic - היא אולי התוכנה הפשוטה ביותר המגינה על שולחן העבודה באמצעות סיסמאות. ניתן להגדיר את התוכנה כך שתנעל את שולחן העבודה אוטומטית, והיא גם מבצעת יומן מעקבים אחר כל ניסיון חדירה חיצוני. תרשים 3.13 מתאר את האפשרויות ש-Black Magic מציעה.

ScreenLock - מאבטחת את הכניסה למחשב באמצעות סיסמה בכמה רמות. ניתן להגדיר את ScreenLock למנוע מ-Windows להתחיל ללא הסיסמה הנדרשת. דוגמה אחת מובאת בתרשים 3.14, ובה המשתמש נדרש לענות לשאלה שהתשובה עליה היא סיסמת המערכת. כמובן, שהתשובה צריכה להיות קשה לניחוש. סיסמה לא צריכה להיות קלה לניחוש.

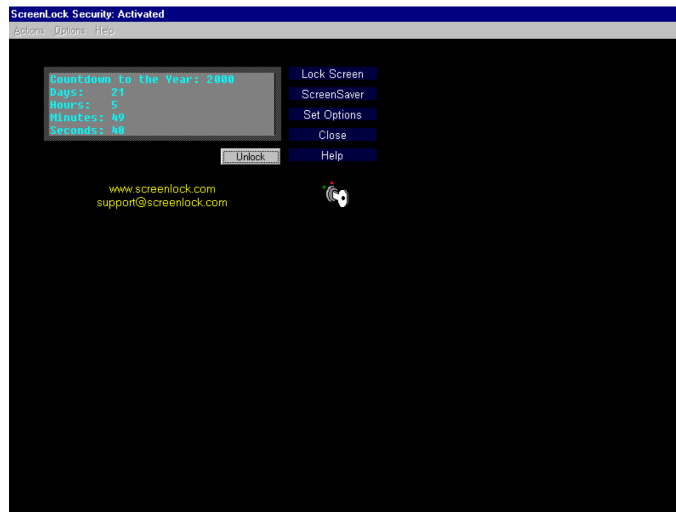


תרשים 3.13 אפשרויות הפעולה של Black Magic.

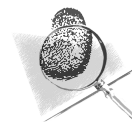


תרשים 3.14 ב- ScreenLock הסיסמה היא תשובה לשאלה, דבר המקל על זכירתה.

בנוסף, ניתן להפעיל את ScreenLock באמצעות מקש **חם** בעת עזיבת המחשב ללא השגחה. כמתואר בתרשים 3.15, ScreenLock גם יכולה לשמש כשומר מסך. ניתן להגדיר את ScreenLock לנהל יומן ניסיונות פריצה שנעשו בהיעדרך מהשולחן שלך.



תרשים 3.15 ScreenLock מתפקדת כשומר מסך וכמנהל יומן ניסיונות פריצה למערכת האבטחה

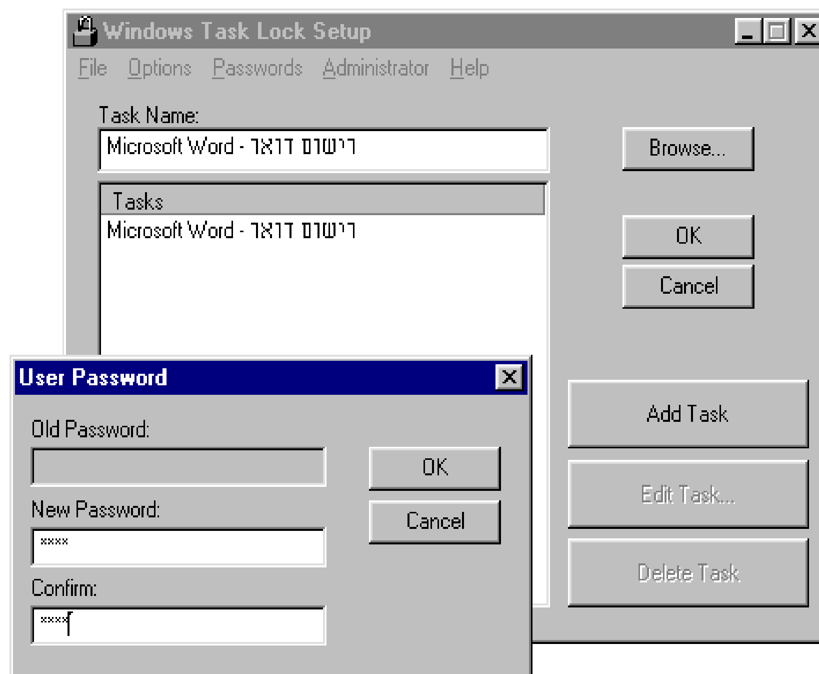


מקש חם הוא צירוף שניים או יותר מקשים, אשר נלחצים בו-זמנית, וגורמים לפעולה או מפעילים תוכנה. דוגמאות אחדות של צירופי מקשים חמים הם Ctrl+I, Alt+M ו-Shift+9.

Windows Task Lock - מספק אמצעי פשוט אך יעיל להגן על יישומים מוגדרים באמצעות סיסמה, ללא תלות באופן הפעלתם. אפשרויות ותכונות הכוללות אירועי קול, מצב פסק זמן חמקן לסיסמה (Password Timeout Stealth Mode), תמיכה רב-לשונית, הפעלה באמצעות מקש חם, והצפנה. תרשים 3.16 מתאר כמה קל להגדיר תוכנת שירות זו.

WinGaurdian - ניתן להגדיר את WinGaurdian לדרוש סיסמה באתחול ל-Windows או להגנה באמצעות סיסמה על כל חלון תוכנה. היא יכולה לחסום תוכנות MS-DOS, ואת מצב MS-DOS עצמו. WinGaurdian מגיע עם 20 חלונות מוכנים להגנת יישומים כגון **לוח הבקרה, מנהל קבצים,** תפריט **הפעלה** וכו'.

WinZip - WinZip, תוכנת הדחיסה והארכיב הנפוצה ל-Windows, מציעה תוכנית הגנה יעילה באמצעות סיסמה. תוכל להגדיר ארכיב כך שהקבצים המתווספים הם מוגני סיסמה, ולא ניתן להסירם או להעתיקם מהארכיב ללא הסיסמה שהגדרת. לתוכנה זו יש כמה יישומים מעניינים ביותר, הנידונים ביתר פירוט בפרק 5.



תרשים 3.16 הגדרת Task Lock עבור חלונות היא פעולה פשוטה.

קבצי ארכיב ו-WinZip

קובץ ארכיב יכול להכיל אחד או יותר קבצים. תכונה יעילה נוספת היא דחיסה, שלעיתים קרובות מפחיתה את גודל הקבצים בארכיב במידה ניכרת, ומכאן שזמן הורדת הקובץ קטן (ופחות מקום נדרש לאחסן אותו).

ישנן מספר צורות של קבצי ארכיב, והנפוצה בהן היא ארכיב מסוג ZIP., שמקורו בתוכנה שיתופית PKZIP של PKWARE. ZIP. הפכה לתקן למעשה לארכיב בעולם המחשבים, המקוון והלא מקוון (ראה /http://www.pkware.com למידע נוסף).

WinZip, תוכנה שיתופית נוספת, היא התוכנה הנפוצה ביותר לפתיחת ארכיבי ZIP. WinZip גם יוצרת קבצי ארכיב המפעילים ופותחים את עצמם כשהם מורצים כתוכנות תחת Windows (ראה http://www.winzip.com למידע נוסף). כמו כן תמצא את WinZip על התקליטור המצורף).

תוכנות מסחריות

תוכנה מסחרית היא תוכנה הנרכשת בחנויות מחשבים ובחנויות אחרות, או באמצעות הדואר, או דרך אתר האינטרנט. פרט לכך שתוכנות אלו אינן חינם, אחד ההבדלים החשובים בין תוכנות שיתופיות למסחריות היא שתוכנות מסחריות נוטות להיראות מקצועיות יותר בהופעתן ואריזתן. לעיתים, תוכנות מסחריות כתובות טוב יותר, אך לא תמיד. לבסוף, תוכנות מסחריות לרוב מיוצרות על ידי חברות בעלות סיכויי הישרדות גדולים יותר בתחום התוכנה, כך שתוכל לסמוך על הוצאת גרסאות ועדכונים חדשים, כולל אחריות על המדיה.

התוכנות הבאות הן מהטובות יותר בתחום זה:

AutoShutdown - מתוצרת Barefoot Productions, היא מן המוצרים המסחריים המעניינים יותר המציעים הגנה באמצעות סיסמה, בנוסף לכמה תכונות מעניינות נוספות.

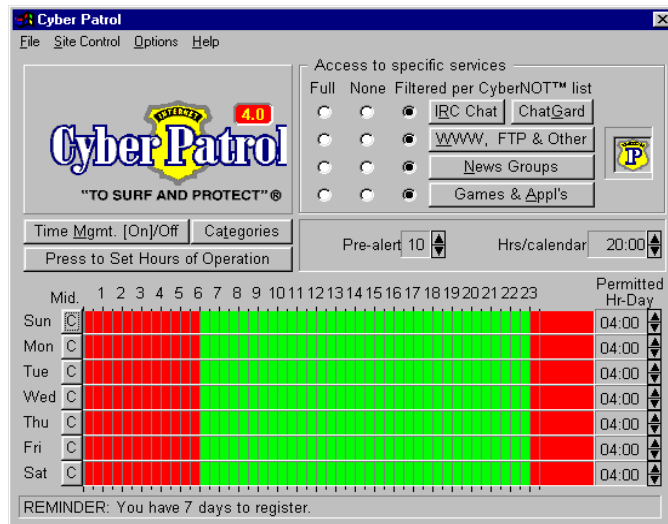
CyberPatrol - היא תוכנת סינון ומעקב היכולה לשמש להגבלת גישה למחשב או לאינטרנט. היא גם עוקבת אחר פעולות של מישהו אחר במחשב שלך (יש לזה ערך אם אתה מרשה לאחרים להשתמש במערכת שלך) בנוסף להגבלת גישה למחשבים. Cyber Patrol מספקת הגנה באמצעות סיסמה למרכיבים שונים של המחשב. ניתן להגדיר את המערכת עד תשעה משתמשים שונים, כל אחד עם שם משתמש וסיסמה ייחודיים. ניתן להגביל כל משתמש לתיקיות ותוכנות מוגדרות. תרשים 3.17 ייתן לך מושג על יכולות Cyber Patrol.

Norton Utilities 2000 - ערכת תוכניות שירות ותיקה זו היא ללא תחרות בתפקוד כללי, במיוחד בנושאי אבטחה. מחיקת קבצים לצמיתות, שחזור קבצים ניזוקים או מחוקים, ותכונות רבות נוספות הן חובה למשתמשים כבדים במחשבים.

החבילה כוללת גם הגנה באמצעות סיסמאות (שים לב שיש גרסאות עבור Windows 95/98 ו- Windows 2000).

Private File - מוצר זה, מתוצרת Aladdin Systems, מספק גישה גרפית להגנה. גרור והשמט קובץ בקופסאות שולחן העבודה המסופקות על ידי Private File, והקובץ ידחס ויוצפן. נדרשת סיסמה מתאימה להצפנה או לפענוח.

Security 98 for Win 95/98 - תוכנה זו ממצבת את עצמה כשומר חמוש של המחשב. Security 98 תוכננה בעיקר להגנה בפני וירוסים, לטפל בעוגיות (Cookies), ולמעקב אחר פעילות משתמש באינטרנט. אולם, היא יכולה גם לבצע הצפנה ייחודית. לצורך העניין, Security 98 גם מציעה תכונה המשמשת להגבלת הגישה לקבצים ותיקיות.



תרשים 3.17 מסך הגדרה של Cyber Patrol

עתה, כשיש לך את הידע הבסיסי הנדרש להגנה על קבציך ופרטיותך על ידי הגדרת סיסמאות וביצוע התאמות פשוטות ל-Windows וליישומים במחשב, תוכל לבחון ביתר פירוט מה ניתן לעשות עם קבצים. פרק 4 מתמקד בכמה תחבולות שבהן תוכל להשתמש להסתרת המידע - ואיך להתגבר על כמה תחבולות שהמידע שלך יכול להפעיל עליך.

פרק 4



הגנה על קבצים ותיקיות באמצעות הסוואה והטעיה

מה בפרק:

- הסוואת תצוגות קבצים ותיקיות ברירת מחדל
- הטעיה באמצעות שמות קבצים וסיומות מטעות
- הטעיה בעזרת קבצים חליפיים
- אמצעי אחסון חיצוניים
- שימוש בארכיבים להסתרת קבצים
- יישומי ארכיב נוספים

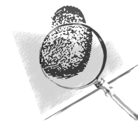
פרק זה בוחן מיגוון דרכים להסוות את קבציך הרגישים, כיסוי עקבות המובילות אליהם, ושימוש ביישומים להחלת סיסמאות ואמצעי הגנה נוספים.

משם, נעבור לאחסון חיצוני וארכיבים, בנוסף לדיון במספר עצות ותחבולות.

הסוואת תצוגות קבצים ותיקיות ברירת מחדל

האימרה הישנה "רחוק מהעין, רחוק מהלב", ניתנת ליישום לגבי קבצים ותיקיות במחשב. בסופו של דבר, אם לא ניתן לראות קבצים ותיקיות מסוימים, איש לא ידע על קיומם, נכון?

אולי. חטטן מיומן ימצא יותר משרצית שימצא, עם מעט ידע, זמן ומוטיבציה. אולם החטטן האקראי, שיש לו גישה למחשב, אינו יודע מה מאוחסן אצלך אם זה אינו גלוי.



בנושא מידע גלוי, ישנן טכניקות ההופכות קבצים ותיקיות לבלתי נראים לרוב היישומים, ולפעמים גם לסייר Windows. אלו יפורטו בהמשך בפרק 5.

בפרק זה נלמד טיפים, תחבולות, וטכניקות ההופכות קובץ כמעט בלתי ניתן לאיתור.

שינוי רשימת קבצים אחרונים שהיו בשימוש

היישומים האהובים עליך משאירים מצביעים ברורים לקבצים חשובים ולמעשיך ביישומים אלה לאחרונה. המצביעים הברורים ביותר הם **רשימת קבצים אחרונים שהיו בשימוש** (Recently Used File List) בתפריט **קובץ** של היישום, כמתואר בתרשים 4.1.



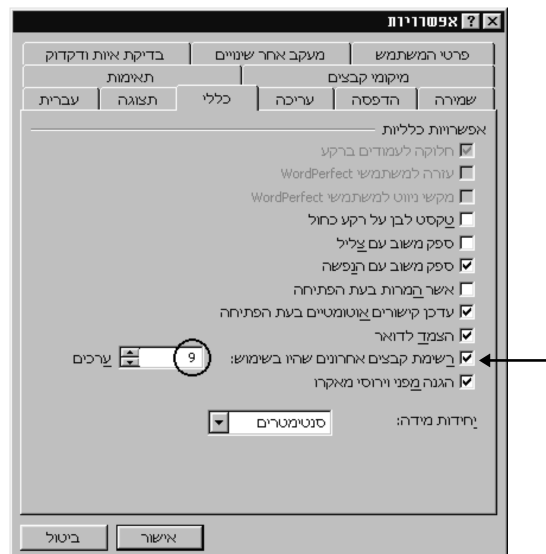
תרשים 4.1 רשימת קבצים אחרונים שהיו בשימוש של Microsoft Word.

רשימה זו מציגה את הקבצים שפתחת לאחרונה לפי סדר, כאשר אלה שנפתחו אחרונים הם בראש הרשימה. זהו כלי נוח אם אתה פותח קבצים מסוימים בקביעות, כיון שהוא מספק קיצורי דרך לקבצים אלה.

רשימת קבצים אחרונים שהיו בשימוש מקלה גם על כל אדם זר לפתוח קובץ שעליו עבדת, ללא צורך לחפש אותו, כיון שהמידע על מיקום הקובץ מאוחסן על ידי היישום ומקושר לפריט הבחירה ברשימה.

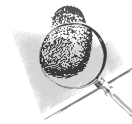
למרות שזה נראה מובן מאליו, ניתן ללמוד די הרבה על מעשיך - אף אם מחקת את הקבצים המופיעים ברשימה. לדוגמה, **רשימת קבצים אחרונים שהיו בשימוש** במחשב המשרדי הכוללת את הקבצים resume.doc, shopping.doc, project8.doc, ו-gifts.doc (מסמכים: קורות חיים, קניות, פרויקט 8, ומתנות) יצביע בבירור שעסקת יותר בענייניך האישיים מאשר בענייני החברה. אי לכך, אולי רצוי לוותר על הנוחות שבגישה מהירה לקבציך האחרונים לטובת פרטיות - דבר הניתן לעשות. יישומים רבים המספקים רשימת קבצים כזו (Microsoft Word, Excel, PowerPoint בין השאר), מאפשרים להגדיר את מספר הקבצים ברשימה מ- 0 עד 9.

להגדרת מספר הקבצים ברשימה, עליך לשנות את אפשרויות התוכנה השולטת בזה. ככלל, ניתן לעשות זאת דרך תיבת הדו-שיח **אפשרויות**, המתוארת בתרשים 4.2. לגשת לתיבה זו, בחר **אפשרויות** בתפריט **כלים,** ולחץ על כרטיסיה **כללי**.



תרשים 4.2 תיבת דו-שיח **אפשרויות** של תוכנת Word.

תיבת דו-שיח זו היא של Microsoft Word (לתוכנות Excel, PowerPoint ואחרות יש תיבות דו-שיח **אפשרויות** דומות). בכרטיסיה **כללי** ישנה אפשרות להגדיר את מספר הקבצים שיוצגו ב**רשימת קבצים אחרונים שהיו בשימוש**. אם תסיר סימון מתיבת הסימון **קבצים אחרונים שהיו בשימוש**, הרשימה לא תוצג כלל.



ככלל, מספר הקבצים ב**רשימת קבצים אחרונים שהיו בשימוש**, היא מ- 0 עד 9. מספר יישומים עשויים להגביל את הרשימה לפחות, אך כל יישומי Microsoft מאפשרים רשימה של עד תשעה קבצים. אין לכך כל קשר למערכת ההפעלה Windows עצמה, שאין לה שליטה על מספר שמות הקבצים שיישום יכול להציג.



כדי לטשטש את עקבות קבציך מעט יותר, הגדר את מספר הקבצים שיוצגו ב**רשימת קבצים אחרונים שהיו בשימוש** ל- 1. אז, בכל פעם שתעזוב את המחשב, הקפד שהקובץ האחרון שפתחת יהיה בעל שם מתאים, או תמים למראה וקשור לענייני עבודה. עקב כך, ניתן יהיה להסיק שעבדת רק על קובץ זה.

הטעיה באמצעות שמות קבצים וסיומות מטעות

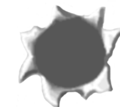
אם ברצונך להטעות עוד יותר בנושא מיקום המידע שלך, שקול שימוש בשמות קבצים שאין להם קשר לתוכן הקובץ. לדוגמה, אם יש לך קובץ בשם Resume.doc (קורות חיים), שנה את שמו ל-Visit In The Zoo.doc (ביקור בגן החיות); או השתמש ב-calender.xls (לוח שנה) במקום budget.xls (תקציב).

לכך יש שני יתרונות. תחילה, השם עצמו מטעה. שנית, אם תבחר סיומת קובץ שהיישום אינו יכול "לראות", כל אדם המחטט באמצעות מעבד תמלילים, גיליון אלקטרוני או כל יישום אחר, לא יוכל לראות קובץ זה אף הוא. Word מחפש קבצים עם סיומת doc. , Excel עם xls. ו- PowerPoint - ppt.. לעיתים קרובות אני משתמש ב-DLL., ששום יישום אינו מכיר כאחד מקבצי המקור שלו, ורוב האנשים יתעלמו ממנו.

להלן התהליך שלב אחר שלב:

1. פתח את **סייר Windows** ונווט לתיקיה בה שוכן הקובץ הרצוי.
2. לחץ לחיצה ימנית על שם הקובץ.
3. בחר **שנה שם** בתפריט שיופיע.
4. הקלד את השם החדש של הקובץ (שם קובץ וסיומת).
5. הקש Enter.
6. תקבל הודעה "אם תשנה סיומת שם קובץ, הקובץ עשוי להפוך לבלתי שמיש. האם אתה בטוח כי ברצונך לשנותו?" לחץ **כן**.

שימוש בתחבולה זו דורש שתזכור את שמות וסיומות הקבצים המשמשים אותך. אם אתה נעזר בסייר Windows כדי לפתוח את הקובץ, יהיה עליך לחזור ולשנות את שמות קבצים אלה לשמם המקורי לפני פתיחתם. אם לא תחזור ותשנה את שם הקובץ לפני שתבחר בו, מירב הסיכויים שתקבל תיבת דו-שיח **פתיחה באמצעות**, השואלת לאיזה יישום אתה רוצה לשייך את הקובץ. כיון **שאתה** יודע באיזה יישום יצרת קובץ זה, תוכל לעלעל במורד הרשימה עד שתאתר את היישום המתאים. כל אדם אחר שיבחר קובץ זה, יצטרך לנחש מה היישום או התוכנה המתאימים לו.



אל תניח את רשימת השמות הנסתרים של קבציך ליד המחשב שלך. מישהו עלול למצוא אותה, ובכך יתבטל אמצעי אבטחה זה.



ניתן לשנות את סיומת ברירת המחדל שבה יישומים שומרים קבצים. הדוגמה הבאה תראה לך כיצד עושים זאת ב- Word 97. לחץ על **קובץ**, בחר את **שמירה בשם**. בתיבת הדו-שיח **שמירה בשם** לחץ על לחצן **אפשרויות**, וגש לרשימה-הנפתחת של **שמור קבצי Word כ:**. בחר את סוג הקובץ כרצונך.

ודא שאינך מגדיר בתיבת הדו-שיח **פתיחה** את השדה **קבצים מסוג** לסוג קבצי הסתר שלך, כיון שאז **יוצגו רק** קבצי הסתר. כמו כן אל תגדיר את **קבצים מסוג** לקבצי All Files (**כל הקבצים**).

הטעיה באמצעות תיקיות חלופיות

לרוב היישומים יש תיקיות **עבודה** (או **ברירת מחדל**) מסוימות, אליהן הם ניגשים בעת פתיחת קובץ. תכונה זו מקלה מאוד על מציאת קבציך, כיון שרוב האנשים נוטים לחפש דברים במקום בו הם מצפים למצוא אותם. (לדוגמה, רוב החטטנים יחפשו תיקיה LETTERS אם ירצו לחפש מכתבים. יש להניח שלא יחפשו מכתבים בתיקיה DOSUTIL.)

כיון שכך הדבר, רצוי להניח את קבציך בתיקיה שאינה ברירת המחדל. כמו כן עליך להימנע מתיקיות ברורות כמו **המסמכים שלי (My Documents)**.

במקום זאת, שמור את קבציך בתיקיה בעלת שם שאינו מתייחס למהות הקבצים. תוכל לדוגמה, ליצור תיקיה בשם UTIL או SYSTEMA בכונן C כתיקיית העבודה שלך. בו בזמן, השאר את תיקיית ברירת המחדל (תיקיית מיקום הקבצים, או תיקיית העבודה, או תיקיה, תלוי ביישום) כמקום בו אינך מאחסן קבצים חשובים.



ניתן לשנות את התיקיה בה יישומים מחפשים את קבציהם (תיקיית ברירת המחדל) באמצעות תיבת הדו-שיח **אפשרויות** או **הגדרות** של התוכנה. בדוגמה של תוכנת Word, ההליך יהיה לחיצה על **כלים**, בחירה ב**אפשרויות**, ולחיצה על **מיקומי קבצים**. עבור Excel, ההליך יהיה לחיצה על **כלים**, בחירה ב**אפשרויות**, ולחיצה על **כללי**, ועבור PowerPoint, ההליך יהיה לחיצה על **כלים**, בחירה ב**אפשרויות**, ולחיצה על **מתקדם**.

יישומים ליצירת קבצים לקריאה-בלבד ומוגני סיסמה

אחת מהתכונות היותר מעניינות של יישום היא היכולת לשמור קובץ כקובץ **לקריאה-בלבד**. כמו כן יישומים רבים מאפשרים הגנת סיסמה על קבצים בעת שמירתם.

שמירת קבצים כקבצים לקריאה-בלבד

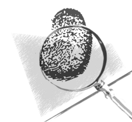
כפי שצוין בפרק 3, קובץ בו הוגדר מאפיין קריאה-בלבד, **לא** ניתן לשינוי אבל **כן** ניתן לשמירה בשם אחר (כמה יישומים לא יאפשרו כל שינוי בקובץ לקריאה-בלבד, בעוד שאחרים יאפשרו שינויים אך לא יאפשרו שמירת השינויים). זו הגנה כנגד שינוי בזדון או בטעות, אם מישהו יפתח את הקובץ ללא ידיעתך. בפרק 3, דנו כיצד להגדיר את מאפיין קריאה-בלבד באמצעות סייר Windows. עתה נראה כיצד לשמור את הקובץ כקובץ לקריאה-בלבד תוך שימוש ביישום שיצר את הקובץ.

לשמירת הקובץ כאשר מאפיין קריאה-בלבד מוגדר מתוך היישום, עקוב אחר השלבים הבאים:

1. בעוד הקובץ פתוח, בחר בתפריט **קובץ**, ולחץ על **שמירה בשם** של היישום. תיבת הדו-שיח **שמירה בשם** תופיע.
2. הכנס את שם הקובץ בתיבת הטקסט ולחץ על לחצן **אפשרויות**. תיבת הדו-שיח **שמירה** תופיע, כמתואר בתרשים 4.3 (אם זה קובץ שכבר נשמר או נפתח שנית, פשוט השתמש בשם הקובץ המופיע בשדה **שם קובץ**, או לחץ על שם הקובץ הנוכחי).
3. לחץ על תיבת הסימון **מומלץ לקריאה-בלבד** בצד הימני תחתון של תיבת הדו-שיח **שמור**. לחץ **אישור**, ואז לחץ על לחצן **שמור** בתיבת הדו-שיח **שמירה בשם**.



תרשים 4.3 תיבת דו-שיח **שמור בשם** פתוחה להגדרת אפשרויות.

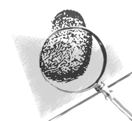


הגדרת קובץ לקריאה-בלבד *אינה* מגדירה סיסמה. כל אדם הפותח קובץ זה יכול לשנות את מאפיין **לקריאה-בלבד**, אלא אם תבצע הגנת סיסמה על הקובץ כמפורט בסעיף הבא.

הגנת סיסמה של קבצים תוך כדי שמירה

אם ברצונך להגן על קובץ בעזרת סיסמה, עקוב אחר השלבים שלהלן:

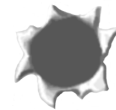
1. מתפריט **קובץ** בחר **שמירה בשם**. תיבת הדו-שיח **שמירה בשם** תופיע.
2. לחץ על לחצן **אפשרויות**.
3. בתיבת הדו-שיח **שמירה** (תרשים 4.3), הכנס סיסמה בשדה **סיסמה לפתיחה**. כאפשרות, ניתן להכניס סיסמה בשדה **סיסמה לשינוי**. זה מאפשר להגדיר רמות גישה שונות לקובץ - לצפייה או לעריכה.



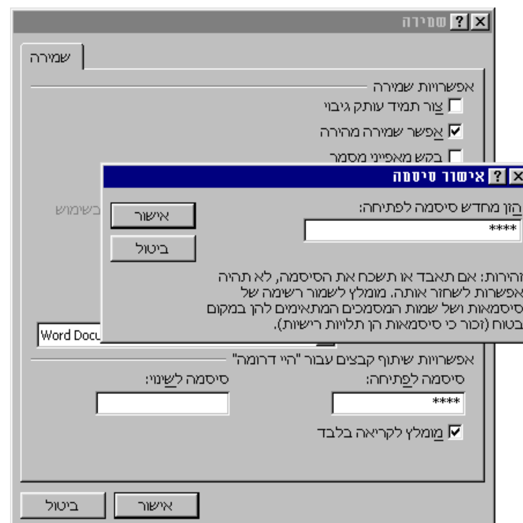
אם תעתיק או תזיז קובץ שבו מאפיין הוגדר ל**קריאה-בלבד**, ו/או הוגדרה הגנת סיסמה על ידי היישום ששימש ליצירת הקובץ, המאפיין או מילת הסיסמה נשארים עם הקובץ (זה נכון גם אם תעתיק את הקובץ עם שם חדש).

4. לאחר הכנסת הסיסמה, תתבקש להכניסה שנית לאימות, כמתואר בתרשים 4.4.

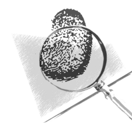
סיסמאות יכולות להיות מורכבות מאותיות או ספרות. אותיות בסיסמאות הן רגישות לאות גדולה/קטנה (Case Sensetive), והמשמעות היא שאם תשתמש באות רישית (אות גדולה) ביצירת הסיסמה, עליך להשתמש באות רישית גם בעת הקלדת הסיסמה לפתיחת המסמך.



שמירת קובץ **לקריאה-בלבד** או קובץ מוגן סיסמה בעזרת היישום שיצר אותו, אינו מגן עליו לחלוטין. ברוב המקרים ניתן עדיין לקרוא (לעיין) בקובץ באמצעות יישומים אחרים - כולל תוכנת עריכה פשוטה. עוד נדון על כך בהמשך בפרק 6.



תרשים 4.4 אימות סיסמת קובץ שנוצרה זה עתה.



שוב, טכניקות אלו נועדו להגן על קבציך מאנשים בעלי ידע מועט או בינוני במחשבים. אם הרגשתך שהטכניקות המתוארות כאן אינן מספיקות להגנת קבצים ו/או תיקיות רגישות במיוחד, שקול שימוש בסיסמאות הגנה נוספת - כמפורט בפרק 3.

אחסון חיצוני וארכיבים

לקבצים רגישים במיוחד ולקבצים שברצונך להשתמש בהם במקום אחר, אחסון חיצוני, מחוץ למערכת (כלומר, לא על הדיסק הקשיח במחשב) הוא הדרך הנכונה. אחסון חוץ מערכתי יכול להיות על דיסקטים, דיסקים בנפח גבוה (כונני ZIP או אחרים), או אף על קלטות או תקליטורים. אני **לא** מציע לך לאחסן קבצים באופן מקוון - באחד מאתרי האינטרנט המציעים אחסון חינם של קבצים (כולל altavista.com) או, אם אתה משתמש בשירות מקוון כספק שירותי אינטרנט (ISP), בשטח האחסון המקוון שלך (איני ממליץ זאת, אך רבים נוהגים כך).

אם אתה מאחסן אחד או יותר קבצים מחוץ למערכת, עליך לשקול להכניס את הקובץ לארכיב. ארכיב היא שיטה מצוינת לניהול קבצים ואחסונם בצורה דחוסה.

אחסון על דיסקט

דיסקטים הם למעשה אחסון חוץ מערכתי של קבצים. לכל מחשב יש כונן דיסקטים אחד או יותר, ודיסקטים ”3.5 אינם יקרים, הם לא כל כך אמינים, ואינם תופסים מקום רב. עקב תכונות אלו, דיסקטים אידיאליים לאחסון מידע רגיש. כאשר נדרש לעיין, לערוך, להדפיס או לגשת לקובץ מכל סיבה אחרת, ניתן לעשות זאת מהדיסקט או להעתיק את הקבצים הנדרשים לדיסק הקשיח באופן זמני (אל תשכח להעתיק קבצים שערכת חזרה לדיסקט ולמחוק אותם על הדיסק הקשיח).

אמורים כבר להיות לך גיבויים של קבציך החשובים על דיסקטים (אם לא, גבה מידע זה עכשיו!). העתקת קבצים היא פעולה פשוטה ביותר, בין אם אתה עושה זאת מתוך סייר Windows, או תוכנית שירות מיוחדת להעתקה/גיבוי.



אל תתפתה לא להדביק תוויות על דיסקטים לאחסון חוץ מערכתי מכיון שאתה בטוח שתזכור את תוכן הדיסקט. מהר מאוד יצטברו לך 10 או 20 דיסקטים ללא תוויות, וכל פעם שתרצה דבר מה מאחד הדיסקטים, תבזבז זמן בעיון בתיקיות של כל דיסקט. הדבק תוויות על הדיסקטים! מצד שני, זכור שהכתוב על התווית עלול להסגיר את תוכן הדיסקט.

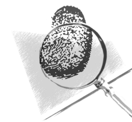
החיסרון האמיתי היחיד כאן הוא הנפח של 1.4MB של דיסקטים ”3.5 סטנדרטיים, העשוי להוות מגבלה אם יש לך מספר קבצים גדולים (או הרבה קבצים קטנים). שימוש בארכיבים, הנידון בקרוב בהמשך, יכול לעזור.



אם אתה מגבה או מאחסן נתונים מחוץ למערכת לעיתים קרובות, שקול יצירת **שני** העתקים של כל דבר על דיסקטים נפרדים. זה "ביטוח טוב" כנגד כשל דיסקט (זה אכן קורה), הרס נתונים, או איבוד או נזק לדיסקטים.

כונני ZIP

כונני ZIP הופכים במהרה לתקן למשתמשי מחשב רבים, וכציוד סטנדרטי במחשבים חדשים. כונני ZIP אינם זולים, אך מימדיהם קטנים יחסית ויש להם יתרון גדול על פני דיסקטים: הם יכולים לאחסן 100MB.



אין כל קשר בין כונני ZIP וקבצי ZIP, פרט לשם. החברות המייצרות קבצים עם סיומת ZIP, נפרדות לחלוטין מ- IOMEGA, החברה המייצרת כונני ZIP ודיסקים.

כשלרשותך כל כך הרבה שטח, אינך צריך לדאוג לעבור לדיסק שני מייד. אולם, ייתכן שתופתע מהמהירות בה קבצים מצטברים ל-100MB. היישומים של היום יוצרים קבצים גדולים מאוד. כמה סוגי קבצים, גרפיים בעיקר, גדולים מעצם טבעם. כך שתאלץ להשתמש בשניים או אף שלושה דיסקים של ZIP לאחסון - בלי למנות את הגיבויים - יותר מהר משאתה חושב.

כיום, החסרון העיקרי של דיסקי ZIP לאחסון חוץ מערכתי הוא עלות. דיסקים של ZIP עולים פי 40 עד 50 ממחיר דיסקטים. בנוסף, אם המחשב אינו כולל כונן ZIP, תאלץ לרכוש כונן. אך למעט חסרונות אלו, דיסקים מסוג ZIP, יותר אמינים מדיסקטים, ודיסק ZIP אחד מחליף עד 70 דיסקטים.



כאשר אתה רוצה להעתיק מספר רב של קבצים לאחסון חוץ מערכתי, שקול שמירת קבצים אלה בתיקיה אחת, שנוצרה למטרה זו. קרא לתיקיה COPY (או כל שם אחר שתרצה), וכאשר תרצה להעתיק את תכולתה, פשוט העתק את התיקיה כולה (זאת מתוך הנחה שיש די מקום לתכולת התיקיה בדיסקט או בדיסק ZIP אליו אתה רוצה להעתיק).

גיבוי על קלטות

גיבוי על קלטות, שפעם היווה את התקן לגיבוי נתונים חשובים שלא יכולת להרשות לעצמך שיאבדו, משמשים עדיין הרבה אנשים, אך הפופולריות שלהם בירידה. בכל זאת, יש להם מקום, למטלות כמו גיבוי המערכת כולה. אולם, גיבוי על קלטות אינה האפשרות הטובה ביותר עקב היותם מגושמים ויקרים מדי למשתמש המחשב המצוי.

אחסון על תקליטורים

כונני תקליטורים וצורבים הם היום ציוד זמין בעלות סבירה, ועקב כך תקליטורים הם, נראים כמדיית אחסון חוץ מערכתית אידיאלית. זה לא בדיוק כך. תקליטורים אידיאליים לקבצים שאינך מתכוון לערוך או לשנות, אך הם אינם מעשיים למידע

שאתה משתמש ומשנה (עורך) תכופות. לאחר שהמידע נצרב על תקליטור, לא ניתן לשנותו ללא התוכנה המקורית, ואז נדרש לחזור על תהליך הצריבה כולו.



אל תזניח אחסון פיסי בטוח למדיית האחסון החוץ מערכתית שלך. חום ולחות עלולים להזיק לדיסקטים ולקלטות ולהופכם לבלתי שמישים. דיסקטים ומדיה אחרת רגישים לנזק פיסי גם כן. יחד עם זאת, קח בחשבון שתרצה לשמור את הקבצים החוץ מערכתיים בטוחים מגילוי.

שמירה מקוונת של קבצים

לאלה מכם החדשים לעולם המקוון, הרעיון של אחסון מקוון של קבצים אולי יישמע מוזר, או אף בלתי אפשרי. הרעיון בר ביצוע ויש אתרי אינטרנט המתמחים באחסון קבצים (אישית, איני סומך על אלה, כיון שקבצים המאוחסנים כך הם מחוץ לשליטת הבעלים, ביותר ממובן אחד. האקרים (Hackers) עלולים לפרוץ לאתר האינטרנט ולמחשב המארח שלו, לגשת לקבצים, להזיק להם או למחוק אותם. עובד באתר עשוי לעשות נזק בזדון, או, האתר עלול להיעלם יום אחד, יחד עם קבציך).

אם אתה מחובר לאינטרנט דרך ISP (ספק שירות האינטרנט), תמצא שהוא הקצה שטח אחסון אישי מסוים - ללא דרישות תוכנה ייחודיות.

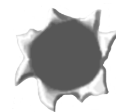
אם אתה משתמש בספק שירות אינטרנט רגיל אשר ההתחברות אליו היא באמצעות חיוג, והספק מציע שטח לדפי אינטרנט אישיים, תוכל להקים דף בית אישי ולהשתמש בשטח זה לאחסון קבציך. כל שנדרש היא תוכנת File Transfer Protocol) FTP, פרוטוקול העברת קבצים) פשוטה להעלאה והורדת קבצים לשטח האחסון המקוון וממנו.



צריך תוכנת FTP טובה למחשב? נסה את WS_FTP. היא זמינה להורדה באתרים רבים וכלולה בתקליטור המצורף לספר זה.

אם כל זה נראה מסובך מדי, או לא מעשי מסיבה אחרת, יש עוד אפשרות אחת: שגר קבצים לעצמך באמצעות דואר אלקטרוני; ואף טוב מכך, שגר קבצים בדואר אלקטרוני לכתובת דואר אלקטרוני שנייה.

אין לך שני ספקי אינטרנט או שירותים מקוונים? אתרי דואר אלקטרוני חינם, כגון Excite או AltaVista, מאפשרים צירוף קבצים לדואר אלקטרוני שאתה שולח או מקבל. בעלות על שני חשבונות דואר אלקטרוני מאפשרת לשלוח קבצים מחשבון A לחשבון B, ולאחסן אותם בחשבון B. בעלות על שני חשבונות דואר אלקטרוני יעילה גם כיון שכמעט לכל ספק שירות אינטרנט, שירות מקוון, ושירות דואר מבוסס אינטרנט יש הגבלת גודל קובץ שלא תוכל לעבור. כמובן, ששידור קבצים כארכיב ZIP יכול לפתור בעיה זו. עיין בסעיף הבא, "אחסון קבצים בארכיב", לפרטים.

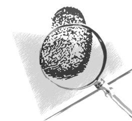


באחסון מקוון של קבצים ישנן שלוש בעיות פוטנציאליות: תחילה, גישתך עלולה להיות מוגבלת עקב בעיות התחברות עם המערכת כתוצאה מתקלות בקווי הטלפון או במערכת המארחת. שנית, אתה עלול לאבד את קבציך עקב תקלה בתוכנה או חומרת המארח. שלישית, הם חשופים, לדעתי, לפגיעה מידי גנבים באינטרנט (האקרים).

אחסון קבצים בארכיב

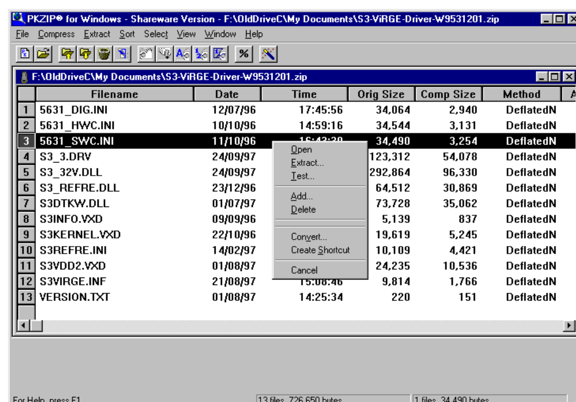
אם בכוונתך לאחסן את קבציך על מדיה ניידת או מקוונת, מומלץ להכניסם לארכיב, מכמה סיבות. אחסון קבצים בארכיב (באמצעות תוכנות PKZIP או WinZip) מכווץ את הקבצים כך שהם תופסים פחות מקום. זה יעיל כאשר ברצונך לשמור מספר קבצים רב (או מספר קבצים גדולים, לפי המקרה) על דיסקט. אחסון קבצים בארכיב משמעו שהם יתפסו פחות מקום - לפעמים 10% מנפחם המקורי.

ארכיב גם מפשט ניהול קבצים. ניתן לאחסן קבצים רבים - 2 קבצים, 10, 50 או יותר - בארכיב אחד אם נדרש, וכך אינך צריך לדאוג להעתקת כל הקבצים ששמרת, לדיסק. בפעולה אחת, ניתן פשוט לפרוש את הקבצים לתיקיה הנדרשת בדיסק הקשיח.

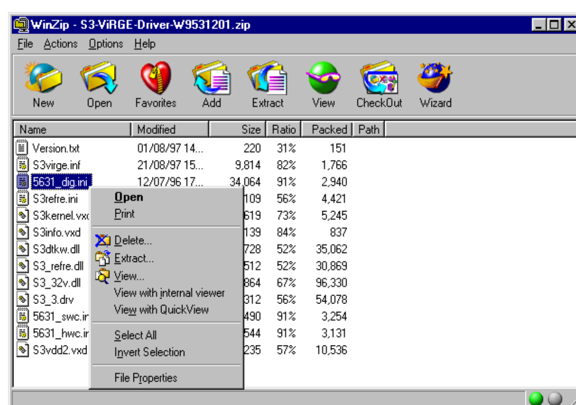


סוגים מסוימים של קבצים אינם נדחסים כמעט או בכלל בארכיב, כגון קבצים גרפיים jpg או gif.

PKZIP ו-**WinZip** הן תוכנות שיתופיות הניתנות להורדה. תמצא את PKZIP ב-http://www.pkzip.com. אתר WinZip נמצא ב-http://www.winzip.com (התוכנות נמצאות גם על התקליטור המצורף לספר זה). משתי תוכנות שיתופיות אלו, נראה ש-WinZip היא בעלת פעולות רבות וקלה יותר לשימוש. אולם, שתי התוכנות הן בעלות תכונות דומות (אפשרויות גרור ושחרר - Drag & Drop, עזרה נרחבת למשתמש, יכולת יצירת קבצי ארכיב לפרישה-עצמית, סריקת וירוסים, עיון ופרישת קבצים מסוימים בלבד מארכיב, ועוד) וגישות שונות למיגוון מטלות. נסה אחת, ואם תגלה שהיא קשה לשימוש או לא ידידותית, נסה את השנייה. כמוזכר, אלו תוכנות שיתופיות, ואינן עולות מאומה בשביל להתנסות.



תרשים 4.5 PKZIP.



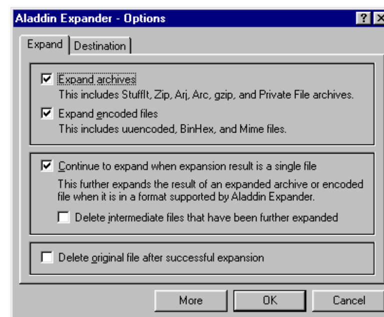
תרשים 4.6 WinZip.

Aladdin Expander, מצד שני, היא Freeware (תוכנת חינם), (כלומר, אינך צריך לשלם כדי להשתמש בה). ניתן להוריד את Aladdin Expander מהאתר http://www.aladdinsys.com. היתרון של Aladdin Expander הוא יכולת הטיפול בקבצים מקודדים בצורת MIME המשמשים תכופות באינטרנט.

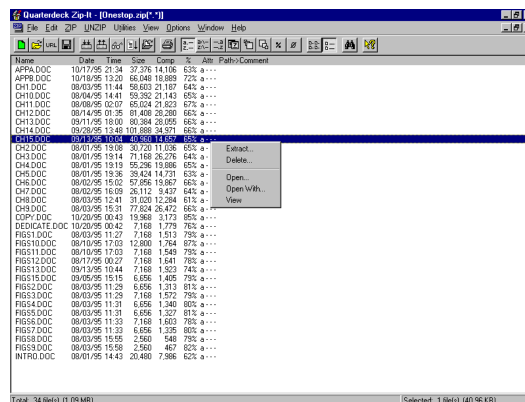
רצוי שתוכנת Aladdin Expander תהיה על שולחן העבודה, אף שעדיין תצטרך תוכנה אחרת ליצירת ארכיבים. בנוסף ליתרונות שצוינו, יש לה גם ממשק ידידותי למשתמש של גרירה ושחרור, כמתואר בתרשים 4.6.

Quarterdeck Zip-It (תרשים 4.7) היא תוכנה קלה יחסית לשימוש המציעה את רוב התכונות שמציעה PKZIP. היא באה עם תוסף תוכנה (Plug-in - תוכנה המתווספת לתוכנה קיימת) הפועל יחד עם Netscape או Microsoft Internet Explorer לטיפול בקבצי ארכיב תוך כדי הורדתם. Quarterdeck Zip-It אינה ניתנת בחינם.

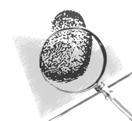




תרשים 4.7 .Aladdin Expander



תרשים 4.8 תוכנת ארכיב Quarterdeck Zip-It.



להוציא מקרים נדירים, תוכנה אחת אינה בהכרח "טובה יותר" מאחרת בעלת תפקוד דומה. לרוב אין "הכי טוב" מוחלט, אלא הטוב ביותר היא החלטה לא סובייקטיבית. תוכנה נתונה יכולה לפעול טוב יותר עבורך ולהתאים לסגנון עבודתך ולצרכיך יותר מאחרות שמכרים ועמיתים ממליצים עליהן בחום. אם תוכנה עבדה עבורך, היא הטובה ביותר. השתמש בה, אך אל תשלול ניסוי דברים חדשים.

רתימת ארכיבים לעבודה עבורך

תוכנה בשם WinZip יוצרת קבצים (עם סיומת ZIP) המכילים קבצים שאינך רוצה שיפלו בידי אחרים. ישנן מספר שיטות לבצע זאת:

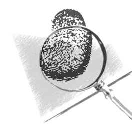
אחסון ארכיבים על הדיסק הקשיח - אם בעלי גישה למחשב שלך אינם אשפי מחשבים, שקול פשוט לשים את כל הקבצים שברצונך להגן עליהם בארכיב אחד או יותר. מקם את הארכיבים בתת-תיקיה קבורה שתיצור, כגון

c:\windows\system\temp\files. הקבצים יהיו בלתי נראים לאנשי מחשבים בלתי מיומנים **בלבד**. תוכל להתקדם שלב אחד הלאה, על ידי מתן סיומת שונה לארכיב, כגון DLL, או RFX - מה שתרצה - כפי שנידון קודם.



אם תרצה לשמור את תוכנת WinZip מחוץ להישג ידם של אנשים לא מורשים, אל תשאיר קיצורי דרך/סמלים על שולחן העבודה או הפניה בתפריט **התחלה** לתוכנה כמו WinZip או PKZIP. במקום, מחק קיצורי דרך והסר את ההפניה האמורה מתפריט **התחלה**. כאשר תרצה להפעיל את התוכנה, השתמש ב**הפעל** מתפריט **התחלה** (ראה בפרק 3, פרטים כיצד להוריד קיצורי דרך ובחירות מתפריט **התחלה**).

אחסון ארכיבים חוץ מערכתיים - אם המחשב שלך נגיש לאנשים היודעים כיצד לפתוח קבצי ZIP, בבית או בעבודה, עליך להסיר את כל הקבצים לאחסון חוץ מערכתי. גם כאן שימוש בארכיב יהיה יעיל ויקטין את השטח הנדרש לאחסון קבצים חוץ מערכתי.

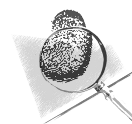


הכנסת קבצים לארכיב מסייעת בהגנה נגד הרס נתונים. יש יותר סיכוי להרס קבצים על דיסקט שאינם בארכיב מאשר קבצים בארכיב. כמובן, הרצוי ביותר זה לשמור **שני** העתקים של כל דבר בארכיב, על שני דיסקטים נפרדים.

דחיסה ופרישת ארכיבים - הכנסה/הוספה לקובץ ZIP ופרישת קובץ ZIP

כמו בכל דבר הקשור למחשבים, קבצי ארכיב ותוכנות ארכיב כוללות שפה סתומה ומונחים רבים. להלן תקציר: כאשר אתה מכניס קובץ לארכיב, זה נקרא "יצירה/דחיסה" (באנגלית: "אריזה" - "compresing"/"Packing") של ארכיב; הוצאת קבצים מארכיב מכונה "פרישה" או "הוצאה" של קבצים (באנגלית: "unpacking" או "extracting" - הוצאה מאריזה, או חילוץ/שליפה). בארכיב ZIP, דחיסה ופרישה נקראים Zipping ו-Unzipping.

כפי שצוין, יש להניח שתשתמש ב-PKZIP או WinZip ליצירת ארכיבים ופרישת קבצים מארכיבים. למרבה המזל, הליכים אלה הם אינטואיטיביים בשתי התוכנות. עצה אחת בנוגע ליצירה, הוספה, ופרישת קבצים מארכיבים: לא מומלץ ליצור או לפרוש קבצי ZIP גדולים על דיסקט. התוכנות לפעמים צורכות יותר מקום משיש על הדיסקט כדי לבצע את עבודתן. רצוי להעתיק את הארכיב מהדיסקט לדיסק הקשיח לפני ביצוע פעולה כלשהי עליו עם הארכיב.



אם אתה מתכוון להוריד קבצים מאתרי אינטרנט או שירותים מקוונים, תמצא שלא תוכל לעבוד ללא PKZIP או WinZip. רוב קבצי התוכנה והמידע המקוונים נמצאים בפורמט ZIP, כיון שזה מפחית את זמני ההורדה ומספק את הנוחות שבשידור מספר קבצים, הנדרשים על ידי רוב היישומים, בהורדה אחת.

כפי שאתה רואה, הסוואה והטעיה, יחד עם אחסון חוץ מערכתי, הם עזרי הגנת פרטיות יעילים ביותר. עתה נעבור להגנה מתוחכמת יותר - כולל הסתרה - בפרק 5.

פרק 5



הסתרת קבצים, תיקיות ויישומים

מה בפרק:

- הסתרה "גלויה" של קבצים
- היכת תיקיות וקבצים לבלתי נראים
- מאפייני קובץ - מה משמעותם וכיצד להגדירם
- סייר Windows וקבצים בלתי נראים
- הסתרה ושינוי שמות קבצי תוכנה
- שימוש בארכיבים להסתרה והגנת סיסמה על קבצים
- אמצעי זהירות חשובים בעת שינוי מיקום קבצים, שמות וסיסמאות

בפרק זה, נדון בכמה מהשיטות המורכבות יותר להסתרה ולהסוואת מידע על הדיסק הקשיח .

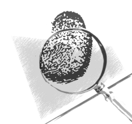
נתחיל בהחבאת קובץ "בצורה גלויה", ונבחן מקרוב כיצד להפוך נתונים, קבצי תוכנה, ותיקיות לבלתי נראים. משם, נדון בכמה טכניקות מיוחדות להחבאת תוכנות, ובשימוש בארכיבים, קבצי Zip להחבאה והגנת נתונים ותוכנות חשובות.

הסתרה "גלויה" של קבצים

אולי הדרך הפשוטה ביותר להחביא קובץ היא להניח אותו במקום שאיש לא יצפה למוצאו. תוכל, לדוגמה, לאחסן קובץ (מסמך) Word או Excel בתיקיית Windows/system/ במקום בתיקיית העבודה של היישום. כך, הקובץ גלוי - עם שם קובץ וסיומת נכונים - אך לעולם לא יתגלה, פשוט כיון שהחטטן **מצפה** שהקובץ יהיה במקום אחר.

רוב האנשים - במיוחד כשזמנם דוחק - לא יחפשו תיקיה אחר תיקיה על מנת לאתר קבצים עם הסיומת והתכנים הנדרשים, ולכן לעולם לא יגלו את הקבצים שהחבאת. אולם, לא תוכל לסמוך על כך שכולם יהיו קצרים בזמן ומוטיבציה, כך שהשארת קובץ "גלוי בחוץ", תחת שמו האמיתי, אינו תמיד הפתרון.

למרבה המזל, יש מספר פתרונות אחרים להחבאת קובץ על הכונן הקשיח. כפי שצוין בפרקים הקודמים, תוכל לשנות שם של קובץ (את תחילת שם הקובץ, או את שם הקובץ והסיומת) או לעשות לו הגנת סיסמה. תוכל אפילו לגרום לקובץ - ולתיקיה בה הוא נמצא - להיות **בלתי נראים**.



אם יש לך דיסק קשיח גדול, הוא עשוי להיות מחולק ללא ידיעתך ל"כוננים" וירטואליים. לדוגמה, דיסק בנפח 3.2GB עשוי להיות מחולק לכונן C וכונן D, כאשר רוב השטח מוקצה לכונן C (עיין במערכת ההפעלה שלך - אתה עוד עשוי להיות מופתע). הכונן שאינו בשימוש הוא מקום טוב להחבאת קבצים - במיוחד קבצים מוצפנים, בהם נדון בפרק 7.

פתאום זה גלוי, פתאום לא: הפיכת קבצים ותיקיות לבלתי נראים

אולי עלה בדעתך שהפיכת קבצים לבלתי נראים היא דרך טובה ביותר להסתירם. אם כן, תשמח לדעת שאכן ניתן להפוך תוכנות וקבצי נתונים לבלתי נראים. הדבר נכון גם לגבי תיקיות.

מה הכוונה ל"בלתי נראה"?

מאפיין Invisible (בלתי נראה) מונע מיישומים "לראות" קובץ (או להציג את שם הקובץ). בתנאים המתאימים, הוא גם מונע מסייר Windows לראות את שם הקובץ. אולם, הקובץ עדיין קיים וניתן להשתמש בו באמצעות פקודות של יישום כל עוד שם הקובץ הנדרש ידוע.

פעולה זו אינה דורשת תוכנה מיוחדת; כמו כן היא אינה דורשת ידע טכני (אף שהסעיף הבא מספק חומר רקע שימושי). אם אתה יודע להשתמש בעכבר, תוכל להפוך כל קובץ נתונים, קובץ תוכנה, או תיקיה לבלתי נראים.

רקע: מאפייני קובץ (File Attributes)

לקבצי מחשב יש **מאפיינים (Attributes)** (מאפיין הוא תכונה או אפיון). בפרק 4, חקרנו את מאפיין **קריאה-בלבד** (**Read-only**), המונע עריכת קובץ. אולם, יש ארבעה מאפייני קובץ בסך הכל, והם:

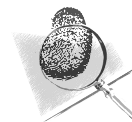
קריאה-בלבד (Read-Only) - מאפיין זה מונע עשיית שינויים בקובץ. אבל לא מונע מחיקתו על ידי סייר Windows וכמה יישומים.

ארכיב (Archive) - מאפיין זה משמש את מערכת ההפעלה לזיהוי קבצים שיש לכלול בגיבוי מערכת ההפעלה.

מוסתר (Hidden) - קובץ מוסתר הוא קובץ שאינו מוצג בתצוגת תיקיה. זה כולל ספריות קבצים ורשימות המוצגות על ידי יישומים. כפי שתלמד, זה כולל לפעמים - אך לא תמיד - רשימות קבצים של סייר Windows.

מערכת (System) - קבצי מערכת הם קבצי מערכת ההפעלה (Windows). ככלל, הם מוגנים נגד מחיקה או שינוי.

למטרותינו, רק המאפיינים ל**קריאה-בלבד** ול**מוסתר** מהווים עניין עבורנו.



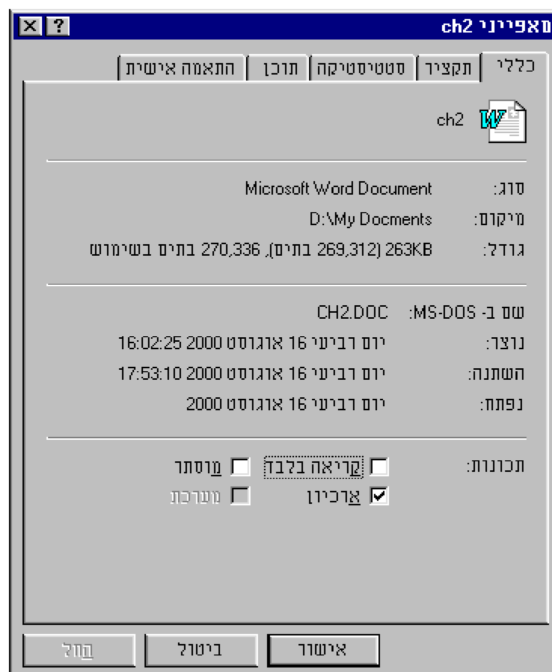
לקובץ ניתן לתת יותר מאיפיון אחד, למשל, הוא יכול להיות גם Read-only וגם System.

הגדרת מאפייני קובץ

מאפייני קובץ ניתן להגדיר באמצעות היישום שיצר אותו, אף שזה אינו נכון לגבי כל היישומים (למדת להגדיר מאפייני קובץ ל**קריאה-בלבד** בפרק 4).

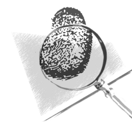
כל מאפיין ניתן להגדרה עבור כל קובץ באמצעות סייר Windows, כדלקמן:

1. לחץ לחיצה ימנית על שם הקובץ שאת מאפייניו ברצונך להגדיר.
2. בחר **מאפיינים** בתפריט המוצג. תיבת הדו-שיח **מאפייני קובץ** תופיע, כמתואר בתרשים 5.1.



תרשים 5.1 תיבת דו-שיח **מאפייני קובץ** עבור קובץ בשם Ch2.doc

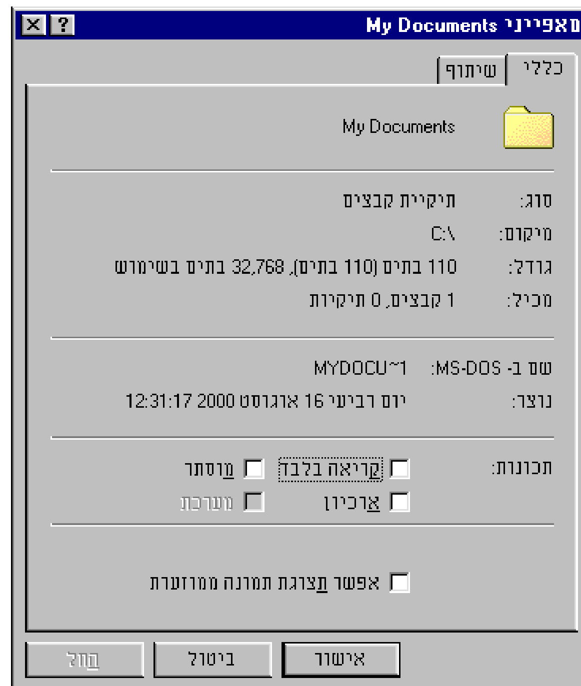
כפי שניתן לראות, המאפיינים מופיעים בתחתית תיבת הדו-שיח. להגדרת מאפיין קובץ, לחץ על תיבת הסימון שלו. להסרת מאפיין קובץ, לחץ והסר סימון מתיבת הסימון שלו.



מאפיינים מוגדרים באופן זהה עבור קבצי נתונים ותוכניות.

הגדרת מאפייני תיקיה

לתיקיות יש מאפיינים זהים לקבצים, כמתואר בתרשים 5.2, המציג מאפייני תיקיה המכילה קבצי מולטימדיה.



תרשים 5.2 תיבת דו-שיח של מאפייני תיקיה בשם My Documents.

ניתן לעיין במאפייני כל תיקיה באמצעות סייר Windows, כדלקמן:

1. פתח את סייר Windows ולחץ לחיצה ימנית על תיקיה כלשהי.
2. בחר **מאפיינים** בתפריט המוצג, ותיבת דו-שיח **מאפיינים** תופיע.
3. להגדרת מאפיין תיקיה, לחץ על תיבת הסימון שלו. להסרת המאפיין, לחץ והסר את הסימון מתיבת הסימון.

שלב הסיום

כדי להפוך קובץ נתונים, קובץ תוכנה, או תיקיה, לאובייקט בלתי נראה על הדיסק הקשיח, עליך להגדיר את מאפיין **מוסתר** בתיבת הדו-שיח **מאפיינים** של האובייקט. לאחר שעשית זאת, הקובץ או התיקיה לא ייראו יותר בתיקיית יישום או רשימה.

אולם אינך בטוח עדיין. נשאר עוד שלב אחד לסיום הפיכת האובייקט לבלתי נראה: עליך לעשות התאמה בסייר Windows.

גם לאחר שהפכת תיקיה לבלתי נראית, תכולתה עדיין גלויה כאשר שם התיקיה נכלל בחיפוש בתיקיה. אולם, אלא אם מישהו יודע על קיום התיקיה, הם לא יוכלו לצפות בקבצים שבתוכה, כיון שלא ידעו מספיק כדי לבצע חיפוש לפי שם (אלא אם הדבר קורה במקרה).

הסתייגות סייר Windows להסתרה

לאחר שהגדרת את מאפיין **מוסתר** לקובץ או תיקיה, לא תוכל לראות את הקובץ או התיקיה באמצעות סייר Windows - אלא אם סייר Windows מוגדר להציג קבצים שהמאפיין שלהם הוגדר **מוסתר.**

כדי לבדוק זאת, פתח את תפריט **תצוגה** של סייר Windows ובחר **אפשרויות.** תיבת הדו-שיח **אפשרויות** תופיע, כמתואר בתרשים 5.3. לחץ על לחצן האפשרויות **הסתר קבצים מסוגים אלה** להסרת הסימון ולאפשר לסייר Windows להציג קבצים מוסתרים ותיקיות; או לחץ על הלחצן כך שימנע מסייר Windows להציג קבצים ותיקיות נסתרים.

אף שהגדרת את סייר Windows כך שלא יציג קבצים נסתרים, ובכך מנעת מאחרים לצפות בהם, המאפיין קל לשינוי כפי שראית. לכן, אם אתה מצפה שחטטן שיש לו יותר ידע במחשבים יניח ידיו על המחשב שלך, קח בחשבון שתחבולה זו לא תמנע ממנו גישה לאורך זמן.

תרשים 5.3 תיבת הדו-שיח **אפשרויות תיקיה** של Internet explorer (במערכת Windows 98) כאשר האפשרות **אל תציג קבצים מוסתרים** נבחרת.

הסתרת יישומים (תוכנות)

הסתרת יישום זו תחבולה יעילה; אם לא ניתן להריץ את היישום שיצר את הקובץ, לא ניתן לראות את הקובץ (בוא נאמר שיותר קשה לראות את תוכן הקובץ). אם תשלב מספר טכניקות שלמדת בספר זה, תוכל להיות כמעט בטוח שאיש לא יוכל לאתר את היישום. השלבים להסתרת יישום פשוטים:

1. הסר את התוכנה מתפריט **התחלה**, כמפורט בפרק 3. אם יש קיצור דרך/סמל עבור התוכנה על שולחן העבודה, מחק אותו (ורוקן את סל המיחזור).
2. הזז את התוכנה וקבציה לתיקיה חדשה. אם יש מחיצות על הכונן, צור את התיקיה החדשה על הכונן המשמש הכי מעט או אינו בשימוש כלל (לרוב כונן D).
3. הפוך את **כל** קבצי התוכנה והתמיכה - **בנוסף** לתיקיה בה הם שוכנים - לבלתי נראים על ידי הגדרת מאפיין **מוסתר**.

ודא ש**רשימת המסמכים** בתפריט **התחלה** ריקה, ושהגדרת את קובץ היישום כ**מוסתר** בעזרת **סייר Windows**. אם לא תעשה כך, מישהו פשוט יכול ללחוץ על הפריט ב**רשימת המסמכים**, או על שם היישום **בסייר Windows**, והתוכנה תופעל מייד.

מה עוד? יש צעד נוסף: שנה את שם קובץ התוכנה למשהו שאינו מרמז שזה תוכנה, כך שגם אם חטטן ייתקל בה, הוא לא יזהה אותה כתוכנה. אולי אפילו שם כמו grazu.exe. אם זה נשמע בלתי סביר, קרא הלאה.

ערכו של שם: הסתרת תוכנות על ידי שינוי שמם

האם השם grazu.exe נראה בלתי סביר לתוכנה? האם הוא כה מוזר שלא ייתכן שיעבוד? נסה בעצמך על ידי ביצוע השלבים הבאים:

1. פתח את **סייר Windows**, ואז פתח את התיקיה **Windows/**.
2. לחץ לחיצה ימנית על שם הקובץ SOL.exe, ובחר **שנה שם** בתפריט שמופיע.
3. הקלד **grazu.exe** או **hodami.exe** והקש Enter.



אם זכור לך בסעיף "הטעיה באמצעות שמות קבצים וסיומות מטעות" בפרק 4, תוכל להשתמש כמעט בכל דבר לסיומת קובץ, כל עוד תזכור לשנות את הסיומת בחזרה לשמה המקורי לפני שאתה עצמך תוכל לפתוח את התוכנה. זאת כיון ש-Windows לא יודעת לאיזה יישום לשייך את התוכנה עד שתאמר לה - או על ידי החזרת הסיומת לברירת המחדל של היישום, או על ידי בחירת התוכנה הנכונה מתיבת הדו-שיח **פתיחה באמצעות**. עיין בפרק 4 לדיון מעמיק יותר בטקטיקה

זו.	
הימנע משינוי שם התוכנה לשם של תוכנה אחרת. שימוש בשם תוכנה אחרת יגרום לכל הפחות לבלבול גדול, ובמקרה הגרוע ביותר, אם התוכנה באותה תיקיה, הוא ידרוס את התוכנה המקורית, ויהפכה לבלתי שמישה לחלוטין.	

4. לחץ פעמיים על השם שהכנסת; המשחק Solitaire (משחק קלפים) יתחיל (אל תשכח להחזיר את השם המקורי, אלא אם אתה רוצה להסתיר תוכנה זו).

שים לב שאם לא שינית את הסיומת, עדיין תוכל להתחיל את התוכנה מתפריט **התחלה**. זאת כיון שהשם הפנימי של קובץ התוכנה לא שונה, ולכן מערכת ההפעלה יכולה לאתר ולהריץ אותה.

אל תשנה שמות של קבצי תמיכה הנמצאים בתיקיה של קובץ תוכנה. זאת כיון שיש תוכנות המחפשות תמיכה לפי שמות תיקיות, ושינוי השם (שם קובץ/או סיומת) יהפכו אותם לבלתי נראים עבור התוכנה.	

שימוש בארכיבים להסתרה והגנה על קבצים

תוכנת WinZip אמורה להיות מוכרת מהפרק הקודם. אם לא, הקדש כמה דקות לקריאה על WinZip והתקן אותה במחשב (הגירסה האחרונה של WinZip נמצאת בתקליטור המצורף לספר זה).

ארכיב כאמצעי הסתרה

בפרק 4, למדנו כיצד להשתמש בארכיב WinZip לאחסון קבצים מחוץ למערכת על דיסקטים בצורה יעילה ובטוחה. ארכיבים של WinZip יכולים לשמש גם לאחסון קבצים על הדיסק הקשיח ואינם ניתנים לאיתור על ידי אנשים שאינם יודעים על ארכיבים ו-WinZip.

לדרגת אבטחה נוספת, שנה את שם קבצי ZIP לשם אחר. תמיד תוכל להחזיר את שם הקובץ בחזרה ל-ZIP.

כמו כן, שקול להסתיר גם את תוכנת WinZip עצמה, באמצעות הטכניקות המפורטות בסעיף "הסתרת יישומים".



WinZip מאפשרת הרצת תוכנות מארכיב. תכונה זו שמישה להגנת תוכנה קטנה שאינך משתמש בה תכופות. הוסף הגנת סיסמה כמפורט בסעיף הבא, ואיש לא יוכל להריץ את התוכנה, אף אם הוא יודע כיצד להשתמש ב-WinZip.

הגנת סיסמה לארכיבים

כפי שצוין, WinZip מספקת הגנת סיסמה לארכיבים. תוכל להוסיף סיסמה בעת יצירת הארכיב או אחר כך. פשוט בחר את הארכיב שעליו ברצונך להגן באמצעות סיסמה, ובחר **Password** בתפריט **Options** של WinZip. תופיע תיבת דו-שיח, כמתואר בתרשים 5.4.

הגנות כפולות ונשנות: ריבוי סיסמאות וארכיבים

ניתן להניח קובץ מוגן סיסמה (כגון קובץ Word מוגן סיסמה באמצעות Word עצמה) בארכיב מוגן סיסמה וליהנות מיתרון ההגנה של שתי הסיסמאות.

בדומה, תוכל להוסיף קבצי ארכיב מסוג ZIP לקובץ ארכיב מסוג ZIP קיים (צעד זה יעיל לארגון הדיסק אם יש לך מספר קבצי ZIP המתייחסים לאותו נושא). אם יש לקובץ ארכיב סיסמה ואתה מניח אותו בארכיב נוסף שכבר יש לו סיסמה משלו, הגנת הסיסמה עדיין חלה (אולם, קבצי ZIP שתוסיף לא יכווצו שנית).

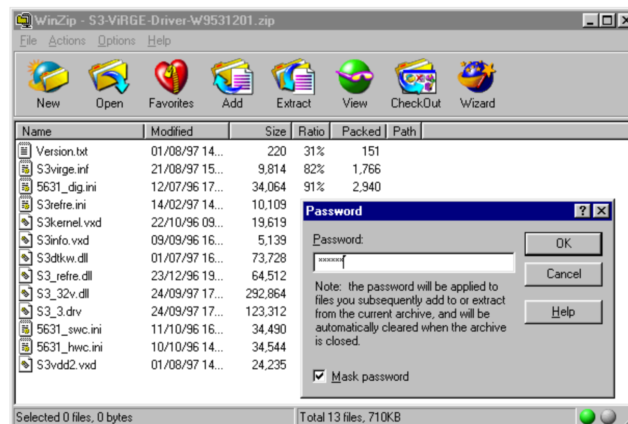
תוכל גם להניח קבצים מוצפנים בארכיב מוגן סיסמה.

כמה אזהרות חשובות

בשלב זה, אתה כבר מוכן להזיז, לשנות שמות, ולהסתיר קבצים - ואת היישומים המשתמשים בהם. לפני שתתקדם יותר מדי בתכנון (או ביצוע) הגנות, זכור שככל שתשנה יותר דברים, כך תצטרך לזכור יותר. שקול כמה תצטרך לזכור כדי לעבור את מחסומי הסיסמאות שהצבת ולאתר את השם המטעה של תוכנות שברצונך להריץ, או למצוא תוכנות וקבצים שהסתרת ו/או הסרת מתפריט **התחלה**.

מידת ההגנה על קבצים תלויה רק בך. אם תרשום מידע זה על נייר כדי לתת תמיכה לזיכרונך, הקפד לשמור את הנייר עליו כתבת את התזכורות על גופך - בארנק וכיוצא בזה. כדאי גם להחביא העתק נוסף, במקרה שתאבד את הראשון. לאחר שימוש חוזר ונשנה בהגדרות החדשות, אתה תזכור את כל מה שרשמת; אך עד למועד זה, אינך רוצה לאבד את הסיסמאות, שמות, ומיקומים שהם המפתח לכל המידע החשוב שלך (ישנן תוכנות המיועדות "לפצח" סיסמאות, אך אין כל בטחון שהן אכן יצליחו).

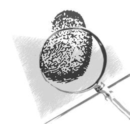
לאחר הגדרת הסיסמה, איש לא יוכל לפתוח, להריץ, לעיין, או לפרוש קובץ מארכיב ללא הסיסמה. ההגנה חלה גם על כל קובץ שיתווסף לארכיב מאוחר יותר.



תרשים 5.4 הוספת סיסמה לארכיב WinZip



אל תבחר סיסמאות פשוטות. כל דבר הקשור אליך אישית (יום הולדת, עיר מגורים, שם ילד, שם משמעותי נוסף, שם חית מחמד, וכן הלאה), אדם שעובד או גר אתך - או פשוט מכיר אותך היטב - יוכל לנחש את הסיסמה. קל יותר לנחש סיסמאות ממה שעולה בדעתך (זה גם אינו רעיון טוב להשתמש בשם המותג של המחשב או קופסת הדיסקטים שעל שולחנך). נסה ליצור מחרוזת תווים אקראית ופעל לזכור מחרוזת זו, במקום לרשום אותה ולהסתכן שמישהו יגלה אותה.



אם נתקלת במושג "כספות" לסיסמאות או תוכנות הגנה אחרות שבהן ניתן לאחסן סיסמאות, מומלץ להימנע משימוש בהן כיון שכך אתה מנית את כל הביצים בסל אחד, אשר ניתן לפרוץ אליו.

עתה, לאחר שלמדת להסתיר את קבציך - במערכת או מחוצה לה - הגיע הזמן להציג מספר קבצים שאולי לא ידעת על קיומם. קבצים אלה, הנוצרים על ידי Windows ויישומים אחרים, נועדו לסייע לך, אך הם גם יכולים להסגיר הכל. נלמד על כך, ועל הרבה יותר מכך בפרק 6.

הסתרת יישומים (תוכנות)

הסתרת יישום זו תחבולה יעילה; אם לא ניתן להריץ את היישום שיצר את הקובץ, לא ניתן לראות את הקובץ (בוא נאמר שיותר קשה לראות את תוכן הקובץ). אם תשלב מספר טכניקות שלמדת בספר זה, תוכל להיות כמעט בטוח שאיש לא יוכל לאתר את היישום. השלבים להסתרת יישום פשוטים:

1. הסר את התוכנה מתפריט **התחלה**, כמפורט בפרק 3. אם יש קיצור דרך/סמל עבור התוכנה על שולחן העבודה, מחק אותו (ורוקן את סל המיחזור).
2. הזז את התוכנה וקבציה לתיקיה חדשה. אם יש מחיצות על הכונן, צור את התיקיה החדשה על הכונן המשמש הכי מעט או אינו בשימוש כלל (לרוב כונן D).
3. הפוך את **כל** קבצי התוכנה והתמיכה - **בנוסף** לתיקיה בה הם שוכנים - לבלתי נראים על ידי הגדרת מאפיין **מוסתר**.

ודא ש**רשימת המסמכים** בתפריט **התחלה** ריקה, ושהגדרת את קובץ היישום כ**מוסתר** בעזרת **סייר Windows**. אם לא תעשה כך, מישהו פשוט יכול ללחוץ על הפריט ב**רשימת המסמכים**, או על שם היישום ב**סייר Windows**, והתוכנה תופעל מייד.

מה עוד? יש צעד נוסף: שנה את שם קובץ התוכנה למשהו שאינו מרמז שזה תוכנה, כך שגם אם חטטן ייתקל בה, הוא לא יזהה אותה כתוכנה. אולי אפילו שם כמו grazu.exe. אם זה נשמע בלתי סביר, קרא הלאה.

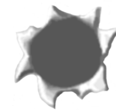
ערכו של שם: הסתרת תוכנות על ידי שינוי שמם

האם השם grazu.exe נראה בלתי סביר לתוכנה? האם הוא כה מוזר שלא ייתכן שיעבוד? נסה בעצמך על ידי ביצוע השלבים הבאים:

1. פתח את **סייר Windows**, ואז פתח את התיקיה **Windows/**.
2. לחץ לחיצה ימנית על שם הקובץ SOL.exe, ובחר **שנה שם** בתפריט שמופיע.
3. הקלד **grazu.exe** או **hodami.exe** והקש Enter.



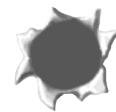
אם זכור לך בסעיף "הטעיה באמצעות שמות קבצים וסיומות מטעות" בפרק 4, תוכל להשתמש כמעט בכל דבר לסיומת קובץ, כל עוד תזכור לשנות את הסיומת בחזרה לשמה המקורי לפני שאתה עצמך תוכל לפתוח את התוכנה. זאת כיון ש-Windows לא יודעת לאיזה יישום לשייך את התוכנה עד שתאמר לה - או על ידי החזרת הסיומת לברירת המחדל של היישום, או על ידי בחירת התוכנה הנכונה מתיבת הדו-שיח **פתיחה באמצעות**. עיין בפרק 4 לדיון מעמיק בטקטיקה זו.



הימנע משינוי שם התוכנה לשם של תוכנה אחרת. שימוש בשם תוכנה אחרת יגרום לכל הפחות לבלבול גדול, ובמקרה הגרוע ביותר, אם התוכנה באותה תיקיה, הוא ידרוס את התוכנה המקורית, ויהפכה לבלתי שמישה לחלוטין.

4. לחץ פעמיים על השם שהכנסת; המשחק Solitaire (משחק קלפים) יתחיל (אל תשכח להחזיר את השם המקורי, אלא אם אתה רוצה להסתיר תוכנה זו).

שים לב שאם לא שינית את הסיומת, עדיין תוכל להתחיל את התוכנה מתפריט **התחלה**. זאת כיון שהשם הפנימי של קובץ התוכנה לא שונה, ולכן מערכת ההפעלה יכולה לאתר ולהריץ אותה.



אל תשנה שמות של קבצי תמיכה הנמצאים בתיקיה של קובץ תוכנה. זאת כיון שיש תוכנות המחפשות תמיכה לפי שמות תיקיות, ושינוי השם (שם קובץ/או סיומת) יהפכו אותם לבלתי נראים עבור התוכנה.

שימוש בארכיבים להסתרה והגנה על קבצים

תוכנת WinZip אמורה להיות מוכרת מהפרק הקודם. אם לא, הקדש כמה דקות לקריאה על WinZip והתקן אותה במחשב (הגירסה האחרונה של WinZip נמצאת בתקליטור המצורף לספר זה).

ארכיב כאמצעי הסתרה

בפרק 4, למדנו כיצד להשתמש בארכיב WinZip לאחסון קבצים מחוץ למערכת על דיסקטים בצורה יעילה ובטוחה. ארכיבים של WinZip יכולים לשמש גם לאחסון קבצים על הדיסק הקשיח ואינם ניתנים לאיתור על ידי אנשים שאינם יודעים על ארכיבים ו-WinZip.

לדרגת אבטחה נוספת, שנה את שם קבצי ZIP לשם אחר. תמיד תוכל להחזיר את שם הקובץ בחזרה ל-ZIP.

כמו כן, שקול להסתיר גם את תוכנת WinZip עצמה, באמצעות הטכניקות המפורטות בסעיף "הסתרת יישומים".

פרק 6



כיצד למנוע מקבציך להסגיר אותך

מה בפרק:

- *מבנה נתוני המחשב*
- *כיצד הנתונים מאוחסנים על הדיסק?*
- *מדוע קבצים מחוקים אינם נעלמים, וכיצד לצפות בהם?*
- *כיצד להיפטר מקבצים מחוקים לצמיתות?*
- *מה חבוי בקבציך?*
- *מה חבוי על הדיסק?*

עתה, לאחר שלמדת כיצד להחביא את קבציך - במערכת ומחוצה לה - נבחן מקרוב את הקבצים עצמם והסכנות הטמונות בהם.

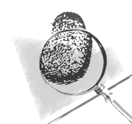
לפני שנדון בכך, נסקור בקצרה כיצד המחשב מטפל במידע ומאחסן אותו. לאחר מכן נבחן כיצד קבצים מאוחסנים על הדיסק, מדוע קבצים מחוקים לא בהכרח נעלמים - וכיצד לוודא שהם אכן נעלמים. מכאן, נלמד כמה דברים מעניינים על תוכן נוסף שמכילים קבציך פרט למידע ששמת בהם.

בנוסף, נגלה כמה קבצים שאולי לא ידעת על קיומם. קבצים אלה, שנוצרו על ידי Windows ויישומים אחרים, נועדו לסייע לך, אך לעיתים הם עלולים לבצע את ההיפך. בהיותם מוחבאים בתת תיקיות על הדיסק הקשיח, הם עלולים לספק מידע רב עליך ועל מעשיך במחשב. נסביר בהמשך כיצד להיפטר מהם.

נתוני מחשב ומבנה נתונים

לפני שניכנס לנבכי הקבצים, נבחן בקצרה כיצד מחשבים מטפלים בנתונים. לא נדון כאן לעומק בעניינים טכניים, ואם אינך רוצה לקרוא את כל החלק הזה, זה בסדר, אך לפחות עלעל בו. אפילו מעט ידע יסייע להשגת מטרותיך (ומי יודע? אולי תמצא עניין רב במידע זה!).

לכל המחשבים המודרניים מכנה משותף אחד - הם מעבדים נתונים **בפורמט דיגיטלי** (ולכן הם נקראים מחשבים דיגיטליים). המשמעות היא שהם רואים ומטפלים בתווי נתונים כ**מחרוזות** (קבוצות) של **ספרות בינאריות**, המוסברות בסעיף הבא.



המושגים **דיגיטלי (ספרתי) ובינארי** משמשים בערבוביה לעיתים קרובות. ובכן, **דיגיטלי** מתייחס לאותות נפרדים מכל סוג שהוא - בינארי או אחרים - שאינם משתנים באופן רציף. במקום זה, אותות אלה מזוהים על ידי שני ערכים או מצבים מסוימים, כגון **מופעל (On)** **ומכובה (Off)**, **שלילי וחיובי**, או **1 ו- 0**. אותות דיגיטליים משתנים מייד ממצב אחד לשני והם אנטיתזה ל**אותות אנלוגיים**, המשתנים לאורך כל הטווח בין שני מצבים אלה. דימוי למצב דיגיטלי יהיה רדיו בעל שני מצבים של עוצמת קול: **גבוה** או **נמוך**. לעומתו, דימוי למצב אנלוגי יהיה רדיו בעל כיוון עוצמת קול רגילה לכל נקודה בין גבוה לנמוך. המושג בינארי יוסבר בסעיף הבא.

בנוסף, כמעט כל המחשבים (למעט כמה מחשבים גדולים) משתמשים בקוד ספרתי זהה לייצוג כל תו - **American Standard Code For Information Exchange** (הנקרא **ASCII**, שיוסבר בהמשך).

נתונים בינאריים

גם אם אין לך נטייה טכנית, בודאי שמעת על מידע המאוחסן ומעובד על ידי מחשבים דיגיטליים ב**פורמט נתונים דיגיטלי** או **בינארי**. אם מחשב משתמש במבנה (פורמט) נתונים בינארי, המשמעות היא שכל **תו** (אות, מספר, סמל, או תו בקרה) שבו מטפל המחשב מעובד ומאוחסן כ**מספר בינארי** מסוים (ישנן כמה סיבות טובות מאוד לכך, אחת מהן תגלה בקרוב).

מספרים בינאריים

מספר בינארי הוא מחרוזת של ספרות דיגיטליות, כגון "1010" או "10011". רק הספרות 0 ו- 1 משמשות בכתב בינארי, בניגוד לספרות 0 עד 9 המשמשות בשיטה העשרונית.

איך מחושב ערך המספר 274 בשיטה העשרונית?

$274=\mathbf{2}x10^2+\mathbf{7}x10^1+\mathbf{4}x10^0=2x100+7x10+4x1=200+70+4=274$

איך מחושב הערך העשרוני של המספר 1011 המיוצג בשיטה הבינארית??

$\mathbf{1011}=\mathbf{1}x2^3+\mathbf{0}x2^2+\mathbf{1}x2^1+\mathbf{1}x2^0=1x8+0+1x2+1x1=8+0+2+1=\mathbf{11}$

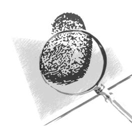
בשיטה העשרונית **בשיטה הבינארית**

שוב, הערך של מספר בינארי נקבע על ידי חיבור הערכים של המקומות המכילים 1. אם יש 0 במקום 1, ערך מקום זה אינו נמנה. טבלה 6.1 מציגה כמה דוגמאות של מספרים בינאריים.

טבלה 6.1: דוגמאות של מספרים בינאריים (דיגיטליים)

ספרה בינארית	ערך עשרוני	ערך עשרוני המיוצג בחזקות של 2
00001	1	2^0
00010	2	2^1
00100	4	2^2
01000	8	2^3
10000	16	2^4
100000	32	2^5
1000000	64	2^6
10000000	128	2^7
...	...	
00110	6	
10001	17	
11111	31	
100001	33	

מטבלה 6.1, קל לראות שהמספר הבינארי 00011 (או 11) זהה למספר העשרוני 3 (חבר את ערכי המקומות: 2+1=3). בדומה, המספר הבינארי 1010 זהה למספר העשרוני 10 (חבר את ערכי המקומות המכילים 1: 8+2=10).



מספר בינארי שלם מכונה לעיתים קרובות **בית (Byte)**. הספרות 1 ו- 0 המרכיבות מספר בינארי מכונות **ספרות בינאריות (Binary Digits)**, הקיצור של מונח זה הוא **סיבית (bit)**. כפי שתלמד, יש שבעה או שמונה bits ב-byte אחד.

מדוע מחשבים משתמשים במספור בינארי?

כפי שהוסבר, רק שני מצבים - **כבוי ודלוק** או **גבוה ונמוך** - נדרשים כדי לייצג מספר בינארי. עקב כך, מספרים כאלה ניתנים לעיבוד מהיר ביותר במחשב, המטפל בנתונים כערכים חשמליים משתנים.

קוד ASCII

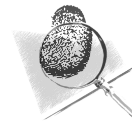
כדי לייצג אותיות, ספרות, ותווים אחרים, ולשלוח אותות בקרה וכו', משתמשים בערכים עשרוניים-בינאריים מוסכמים המייצגים את כל התווים הקיימים. המחשב משתמש בקוד של ספרות בינאריות שהן שוות ערך למבנה הספרות העשרוני. התוצאה היא שהמחשב משתמש במספר בינארי לייצוג כל תו קיים.

בטבלה 6.2 מוצג הערך העשרוני של מספר, הספרה הבינארית המייצגת מספר זה, וכיצד מספר בינארי זה מתורגם על ידי מחשב דיגיטלי (שלוש הנקודות מסמנות דילוג לסדרת מספרים חדשה).

טבלה 6.2: ערכת תווי ASCII

ערך עשרוני	ערך בינארי	תו מיוצג
65	1000001	A
66	1000010	B
67	1000011	C
68	1000100	D
69	1000101	E
70	1000110	F
71	1000111	G
72	1001000	H
...		
103	1101011	g

לדוגמה, ASCII 71 (בינארי 1000111) מייצג את האות G. ASCII 103 (בינארי 1101011) מייצג את האות g. ערכים אחרים מייצגים את שאר האלף-בית (באות גדולה או קטנה), ספרות, סימני פיסוק, רווחים, תווים מיוחדים, ותווים גרפיים. שיטה זו מגיעה עד 255 (11111111), שהוא המספר הבינארי הגדול ביותר המיוצג על ידי 1byte המכיל 8 סיביות (8bits).



כל תו מיוצג על ידי 1byte; מכאן, יחידת המידה של קובץ RAM ומרכיבי מחשב אחרים, היא **קילובייט (Kilobytes)** (או **K**). כל K הוא 1024bytes.

אלה היסודות של טיפול ואחסון נתונים במחשב. עתה נעיף מבט מהיר על אחסון נתונים בדיסקים.

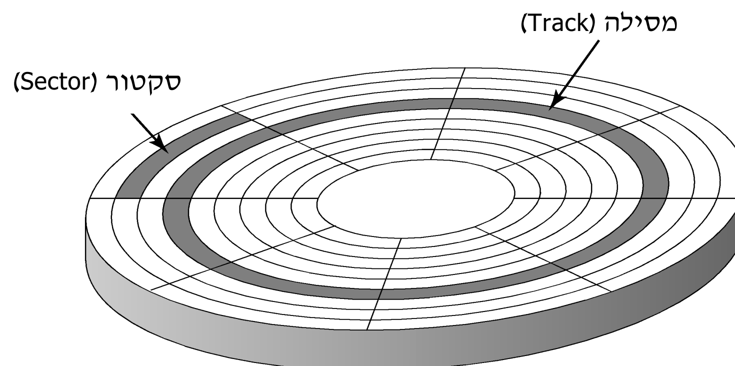
הערה חשובה: תווי ASCII

תווי ASCII מורכבים מתווי ASCII, 0 עד 127. אלה הם תווי בקרה מסוימים, כל אותיות האלף-בית (אות גדולה וקטנה), רווחים, סימני פיסוק, וספרות.

תווי ASCII ממספר 128 ועד 256. אלה תווי בקרה נוספים, תווים גרפיים, בנוסף לתווים מיוחדים כגון ß, ®, ו- ±. פרט לתווים מיוחדים אלה, תווי ASCII מ- 128 ועד 256 אינם מוצגים כרגיל על ידי מעבדי תמלילים ורוב התוכנות האחרות, אף שיש להם ייצוג סמלי הניתן לצפייה על ידי תוכנות מסוימות (ראה דוגמה בתרשים 6.3 בהמשך פרק זה).

כיצד נתונים מאוחסנים על הדיסק

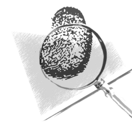
דיסקים של מחשב מכילים חומר מגנטי. נתונים מאוחסנים במחשב, על דיסק קשיח או דיסקט, בתבניות של אזורים ממוגנטים. כל אזור כזה מכונה **סקטור (Sector)**. כל סקטור יכול לאחסן מספר bytes קבוע (לדוגמה, 512 או 256). לפעמים הסקטורים מאורגנים בקבוצות בשם **אשכולות (Clusters)**. סקטורים (ואשכולות) מונחים ב**רצועות (Tracks)**. תרשים 6.1 הוא ייצוג גרפי של סידור זה.



תרשים 6.1 כיצד נתונים מאוחסנים על דיסק מחשב.

למעשה, הדבר החשוב להבנה בדיונים אלה אינו **כיצד** נתונים מאוחסנים, אלא כיצד המחשב עוקב ומאתר **היכן** נתונים מאוחסנים. המעקב מתבצע באמצעות טבלה הנקראת FAT (File Allocation Table). ה- FAT מכיל מידע על כל קובץ - גודלו, היכן הוא מאוחסן, וכן הלאה.

bytes המרכיבים קובץ אינם מאוחסנים לרוב בסקטורים סמוכים. קבצים עשויים להיות מאוחסנים בסקטורים המפוזרים על פני הדיסק. מידע היכן ממוקם כל סקטור עוקב (סמוך או לא סמוך) מאוחסן בסקטור עצמו.

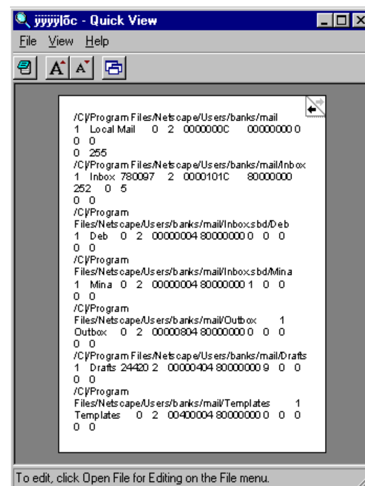


פיזור נתוני קובץ בצורה אקראית על פני סקטורים לא סמוכים אינו יעיל. במידה ויש כמות ניכרת של מידע לא רציף על דיסק, אחזור המידע מואט. לכן רצוי לבצע **איחוי (Defragment)** של הדיסק הקשיח מדי פעם, על ידי שימוש בתוכנית שירות Defrag (איחוי) הכלולה בדיסק הקשיח, או באמצעות תוכנית שירות מסחרית כגון Norton 2000 (איחוי דיסק כרוך בהזזת נתוני כל קובץ מסקטורים פזורים לסקטורים רציפים סמוכים).

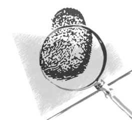
מדוע קבצים מחוקים אינם נעלמים באמת

עתה נגיע לצד מעניין באמת של אחסון קבצים על דיסק: **כאשר קובץ נמחק מדיסק קשיח, הנתונים על הדיסק המרכיבים את הקובץ אינם נמחקים למעשה.** במקום זאת, בטבלת ה- FAT מסומן מקום אחסון הקובץ כפנוי. שם הקובץ לא נמחק מטבלת FAT אלא רק מסומן בצורה שהמערכת "יודעת" שהוא למעשה לא קיים. לאחר מכן, הסקטורים שקובץ זה איכלס זמינים לשימוש, כראות המערכת. עם הזמן הרצועות נדרסות ומשוכתבות על ידי קבצים חדשים, אך הנתונים בסקטורים לא נמחקים או מוסרים.

כך, ישנם סקטורים המכילים את כל הנתונים של קובץ "מחוק". זה טוב כמו קבצים מחוקים, נכון? לא נכון! תוכניות שירות מסוימות, כגון Norton Unerase, יכולות לאתר סקטורים של קבצים מחוקים ולהציגם - ואפילו לאחזרם כקובץ שהמחשב ויישומיו יוכלו לקרוא. זה נכון לגבי דיסקים קשיחים או דיסקטים. תרשים 6.2 מתאר חלק מקובץ מחוק כפי שנצפה באמצעות תוכנית שירות Undelete (שחזר מחיקה). שים לב שתוכנת Norton Unerase מציגה מבט מדויק ככל הניתן של הקובץ המשוחזר.



תרשים 6.2 חלק מקובץ שנמחק, כפי שנראה באמצעות Norton Unerase



אף אם חלק מהסקטורים בדיסק בו אוחסן קובץ מחוק שוכתבו בנתונים מקובץ חדש, עדיין ניתן לראות את שאר נתוני הקובץ באמצעות תוכנית שירות המשחזרת מחיקה. תוכניות שירות Unerase (שחזור מחיקה) מאתרות את כל הקבצים המחוקים שעדיין על הדיסק, ואז מאתרות את כל הסקטורים הקיימים המכילים נתונים מקובץ נתון. תוכניות שירות אלה מאפשרות צפייה בקובץ, ושמירתו כקובץ חדש.

אם אינך עושה שימוש רב במחשב, ואינך יוצר ושומר הרבה קבצים חדשים, רוב הסיכויים שקבצים מחוקים (או חלקים גדולים מהם) יישארו זמינים זמן רב. גם אם אתה משתמש הרבה במחשב , על בסיס יומי, כמה קבצים או חלקי קבצים, יישרדו.

והרי לך - קבצים שמחקת ניתנים לאיתור, צפייה ושחזור. האם ניתן למנוע מאחרים לראות קבצים מחוקים? אם יש להם את הידע והכלים, אז לא, לא ניתן! האם ניתן לסתום פירצת פרטיות זו? כן, עם תוכנית שירות מתאימה, כמפורט בסעיפים הבאים.

איך להיפטר מקובץ מחוק

הפתרון לבעיה של שאריות נתונים מקבצים מחוקים על הדיסק הקשיח או הדיסקט היא לכתוב על הסקטורים שבו היה מאוחסן הקובץ. פעולה זו מכונה לעיתים **איפוס (Zeroing Out)** של הסקטורים, כיון שתוכניות שירות רבות כאלו ממלאות את הסקטור באפסים. כמה תוכניות שירות משכתבות עם נתונים אקראיים, ולרוב ניתן להגדיר להן לשכתב סקטורים מספר פעמים. למעשה יש תקנים של משרד ההגנה האמריקאי המתייחסים להסרת נתונים מחוקים מדיסקים. תוכניות השירות הטובות יותר עומדות בתקנים אלה.

לא ניתן לשכתב או להסיר נתונים מסקטורים ללא אחת מתוכניות שירות אלו. להלן תיאור כמה מהטובות יותר (לתוכניות אלו יש תכונות נוספות שנבחן בפרקים 7, 9, ו- 10).

McAfee Office 2000

אוסף תוכנות שירות זה כולל תוכנות המטפלות בתיקון דיסקים, הסרת תוכנות, וניקוי דיסקים קשיחים. התוכנות יכולות לבצע שכתוב יסודי של שטחי קבצים מחוקים כדי להסיר נתונים לצמיתות.

Norton Utilities 2000

Norton Utilities 2000 היא **התקן** בתחום תוכניות השירות לדיסקים, ועיקר פרסומה נובע מכלי שחזור, מחיקה, ותיקון דיסקים. Norton Utilities 2000 מספקת ערכת כלים לתיקון וניהול דיסקים, וביניהם WipeInfo, תוכנית שירות היכולה להסיר כל זכר של קבצים או תיקיות נבחרות שלמות.

תוכנית השירות Norton WipeInfo יכולה גם "לנגב" שטח חופשי בדיסק הקשיח, ובכך להבטיח שמידע שנמחק בעבר לא נשאר על הדיסק. הטכניקה המשמשת את Norton WipeInfo מתאימה לשיטה המוגדרת על ידי משרד ההגנה האמריקאי.

Quarterdeck Remove-It

תוכנת ניקוי דיסק זו (המסירה גם קבצי אינטרנט מגובים) היא בחירה טובה אם אתה רוצה להבטיח שתוכל לשחזר את מה שמחקת - במקרה וגילית כי טעית (ברגע שתהיה בטוח במה שמחקת, תוכל להשליך את החומר המחוק לצמיתות על ידי ריקון סל המיחזור). כחלק מניקוי הדיסק הקשיח, Remove-It יכולה לשכתב גם מידע מחוק.

תכונות מוזרות של קבצי מעבד התמלילים

תוך התייחסות לאחת הדוגמאות מפרק 1, בוודאי קרה שהקלדת מכתב חשוב וכללת בו מספר הערות שלאחר מכן התחרטת עליהן ומחקת אותן. זה קורה לכל אחד, ובוודאי לא נתת על כך יותר מדי את הדעת לאחר שמחקת את ההערה הנדונה ושמרת את המכתב.

ייתכן גם שהשתמשת במסמך פתוח לכתיבת הערות זמניות - מספר טלפון, מועד פגישה, שם איש קשר, הערות, ומה לא. מחקת את ההערות, השלמת את המסמך ושמרת אותו.

ודאי תופתע לדעת שיש סיכוי טוב שההערות שמחקת מהמכתב עדיין שם; ושההערות הזמניות עדיין במסמך ששמרת ושלחת לאדם אחר. בהתאם למה שעשית במסמכים לפני סיומם, הערות אלו יהיו מביכות, מבהילות או סתם בעייתיות. מצבים אלה מדגימים את הצורך לדעת מה יש במסמכים שלך שחשבת שאין, כיצד להסיר את החומר לצמיתות, וכיצד למנוע ממנו להישאר בעתיד.

או, אולי אתה פשוט סקרן כיצד זה קורה. בכל מקרה, פרק זה יפתח את עיניך.

מה יש באמת בקבצים האלה?

רוב משתמשי המחשב מניחים שמה שיש בקבצים זה מה שהם הקלידו בהם - אותיות, ספרות, סמני פיסוק ואולי גרפיקה. אולם, כמו ברוב הדברים, יש יותר משרואים בקבצים הנוצרים באמצעות רוב יישומי המחשב.

חשוב על מסמך הנוצר באמצעות מעבד תמלילים. בנוסף לתוכן שהוקלד בו, תוכנית מעבד התמלילים גם מאחסנת מידע על מספר רכיבים הקשורים בהגדרת המסמך ובפורמט שלו. בין רכיבים אלה עשויים להיות:

- תווים שלא יודפסו, הכוללים טאבים, Enter ו/או תווי הזנת שורה (הגורמים לתזוזה שורה אחת מטה), וסימני שבירת עמוד
- ריווח שורות ומידע על השוליים
- מידע על הגופנים המשמשים במסמך
- מבני טקסט מיוחדים, כגון טבלאות ורשימות עם תבליטים
- גרפיקה - הגרפיקה עצמה, ונתוני מיקום ומבנה
- קישורים לקבצים אחרים
- הוראות מיוחדות לתצוגה או הדפסה - שורות נוספות בין פסקות, יישור, מרכוז, ועוד.

ברור, אם כן, שיש הרבה יותר נתונים בקובץ מעבד תמלילים משהקלדת (זה גם ההסבר מדוע קבצי מעבד תמלילים הם די גדולים, אפילו עבור מסמך קטן).

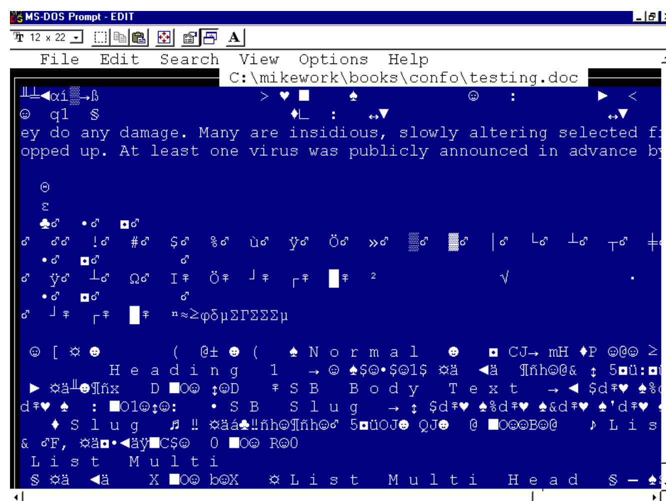
כיצד טקסט מחוק מאוחסן בקובץ

מעבדי תמלילים רבים מאחסנים גם טקסט מחוק בקובץ מסמך (במקרה שתרצה לבטל מחיקה) ולעיתים גם חומר שהעתקת והעברת למקום אחר. זה נכון במיוחד במעבדי תמלילים השומרים את הקובץ לשחזור כנגד אפשרות של הפסקת חשמל או כשל דיסק. לא ניתן לראות חומר זה בעת הדפסת המסמך, ולא כאשר אתה מעיין או עורך אותו באמצעות תוכנת מעבד התמלילים. אולם, הוא שם - ויישאר שם עם הקובץ אף אם תשלח אותו בדואר אלקטרוני או תעתיק אותו עבור מישהו אחר.



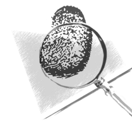
ניתן לשמור מסמך בקובץ ללא כל נתוני הפרמוט, וללא הטקסט המחוק. בעת שמירת הקובץ, בחר סוג קובץ ASCII, Text-Only (טקסט בלבד), או MS-DOS - אחד מביניהם שמעבד התמלילים מציע.

תרשים 6.3 מציג מה באמת מכיל קובץ Word של מיקרוסופט. הצורות המוזרות הם תווים בעלי 8 סיביות או תווים בינאריים המהווים מידע על מבנה המסמך. האותיות והמילים הרגילות הם תווי ASCII רגילים בני 7 סיביות. הם מכונים לעיתים כ- **Literal Characters (תווים כפשוטם)** ומהווים כמובן את רוב תווי המסמך הנוצרים בידי-אדם.



תרשים 6.3 קובץ מעבד תמלילים טיפוסי יכול להכיל נתוני פורמט וטקסט מחוק, בנוסף לתכולתו המכוונת

טקסט מחוק או טקסט ביטול הקלדה שניתן לשחזור (Undo), מאוחסן לרוב בסוף הקובץ. שוב, הודות לקודים מיוחדים בני 8 סיביות, הוא לעולם אינו מוצג על ידי מעבד התמלילים וגם לא בהדפסה.



ככלל, קבצים גדולים וקבצים הפתוחים זמן רב נשמרים לגיבוי - יחד עם הטקסט המחוק - לעיתים קרובות יותר מקבצים קטנים.

אולם, ניתן לעיין בטקסט מוסתר זה על ידי פתיחת קובץ המסמך באמצעות מעבד תמלילים אחר. לעיתים, Windows Wordpad או Notepad יעשו זאת - אף כי קובץ עלול להיות גדול מדי עבור תוכנות אלו. ניתן גם לעיין בקובץ באמצעות תוכנת Edit של DOS (ששימשה להצגת הטקסט בתרשים 6.3).

כיצד להיפטר מטקסט מחוק וטקסט "ביטול הקלדה" ("Undo")

אם אתה רוצה לוודא שטקסט מחוק לא נשמר עם המסמך, יש דרך פשוטה לוודא זאת, ללא צורך אפילו לעיין במסמך באמצעות תוכנה אחרת. עקוב אחר השלבים הבאים:

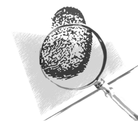
1. שמור את המסמך.
2. צור מסמך חדש (בתפריט **קובץ** בחר באפשרות **חדש** של מעבד התמלילים).
3. חזור ופתח את המסמך המקורי.
4. בחר את המסמך כולו (לרוב דרך תפריט **עריכה**, ולחיצה על **בחר הכל** או על **Ctrl+A**).
5. העתק את המסמך (תפריט **עריכה** ולחיצה על **העתק**).
6. סגור את המסמך.
7. הדבק את התוכן המועתק למסמך החדש שיצרת (תפריט **עריכה** ולחיצה על **הדבק**).
8. שמור את המסמך החדש.

כיון שהעתקת רק את התוכן המוצג מהמסמך המקורי, זה כל מה שהוכנס למסמך החדש.

היכן הסיכון בשיתוף קובץ?

יש להניח שאתה יודע את התשובה לכך לבד. הסיכון שבשמירת קבצי מסמכים ערוכים על הדיסק הקשיח במחשב - או שיתוף קבצים באמצעות דואר אלקטרוני או העתקתם לדיסקט - הוא שאדם סקרן בעל ידע יוכל לראות מה שמחקת בעת יצירת מסמך זה.

אם ברצונך לשתף אדם אחר במסמך כקובץ, צור מסמך חדש והעתק את המסמך המקורי לתוכו. שמור את המסמך החדש ותן את המסמך **הזה**, כיון שהמסמך החדש לא יכיל כל עקבות של חומר שמחקת.



יישומים אחדים כגון גיליונות אלקטרוניים ותוכנות מסדי נתונים, עלולים גם לשמור את מחיקות התווים, מילים ופסקאות. לכן מומלץ להעתיק גם מסמכים שנוצרו על ידי תוכנות אלו אם אתה מתכוון לשתף בהם אחרים.

חור אבטחה גדול - קבצים זמניים

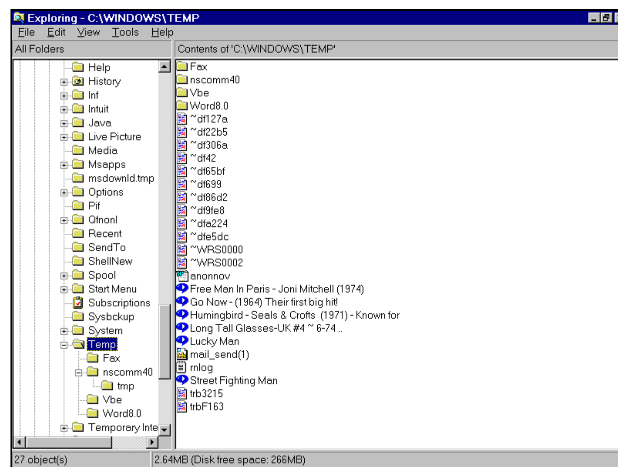
כמו Windows גם Microsoft Word ויישומים אחרים נוהגים לשמור מסמכים בתהליך עשייתם, כנגד אפשרות של קריסת המערכת ו/או כדי לייעל את העבודה. כמה יישומים שומרים גם טקסט שמחקת, הזזת, או העתקת בתוך מסמך. הטקסט נשמר בקבצי דיסק - אף אם לא שמרת את הקובץ שעליו אתה עובד. כאשר תסגור את היישום, כל הקבצים הזמניים אמורים להימחק. הרעיון יפה, אך לעיתים תכונת אבטחה זו אינה פועלת. כך או כך, בסופו של דבר מתקבלים קבצים זמניים חסרי ערך.

תרשים 6.4 נותן מושג על אופן הופעת קבצים זמניים במערכת.

חלק מהקבצים שם עקב בעיית דיסק או נפילת מתח, אך רוב הקבצים הם פשוט שאריות עריכה שהתוכנה שיצרה אותם לא עשתה "ניקיון" כמו שצריך.

ניתן להיפטר מרסיסי קבצים אלה על ידי גישה לתת-התיקיות המתאימות ומחיקת הקבצים הזמניים שיישומים רבים משאירים מאחוריהם. או, ניתן להשתמש באחת התוכנות המסחריות להיפטר מקבצים חסרי ערך אלה.

שווה לבצע ניקוי ידני (המתואר בסעיף הבא) לפחות פעם אחת. אם תשתמש בתוכנה לניקוי דיסקים, תוכל לעבור אחריה כדי לוודא שהיא לא פספסה משהו.



תרשים 6.4 אוסף טיפוסי של קבצים זמניים הממתינים למחיקה, מזוהים בסימן ~ הנמצא לפניהם.

איתור וניקוי ידני של קבצים זמניים

האיתור והניקוי צריך להיעשות לאחר שסגרת את כל היישומים ושורת המשימות - ריקה. התיקיות בהן יש לבדוק קיום קבצים זמניים הם: \Windows\temp וכל תת הספריות מתחת להן בעלות שמות מגוונים כגון \fax או \wordxx. לקבצים יהיו סיומות כמו tmp, אך חלקם יהיו קבצי doc, html או אף קבצי תמונה מלאים, או חסרי סיומת כלל. גודל רבים מקבצים אלה יהיה אפס (0). שמות הקבצים יתחילו לרוב עם סימן ~ כגון: ~wrdtemp.doc. הרשימה בתרשים 6.4 נותנת מושג על שמות אפשריים של קבצים אלה.

לסיכום: חפש קבצים עם סיומת **tmp** ו/או שמתחילים ב- ~.

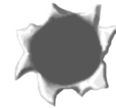
מחק קבצים אלה על ידי בחירתם, ולחיצה על מקש Del; בנוסף לכך שתיפטר מחומר העשוי למשוך חטטנים, יתפנה לך גם שטח דיסק נוסף.



תוכל גם לבדוק קבצים באמצעות Word או Excel, או יישומים אחרים שיצרו אותם. תוכל גם להשתמש בתוכנה גרפית, כגון Paint Shop Pro.

בנוסף, חפש את קבצי הגיבוי הזמניים שיישומים יוצרים כאשר קובץ פתוח. יש להם לרוב שמות כגון ~document.doc, והם יימצאו בספריות העבודה של היישום. הם לעיתים נשארים מאחור ללא סיבה.

השתמש בסייר Windows למחיקת הקבצים. התחל את סייר Windows ונווט לתיקיה שבה הקבצים שברצונך למחוק. למחיקת קובץ, לחץ עליו ואז לחץ על מקש Delete ואשר את המחיקה. אם נדרש למחוק מספר קבצים, תוכל להאיר את כולם ואז ללחוץ על מקש Delete (האר מספר קבצים ביחד על ידי לחיצה על Ctrl ולחיצה על כל קובץ. או בחר קובץ אחד, לחץ והחזק את מקש Shift בעודך נע מטה ברשימת הקבצים באמצעות מקשי החיצים).



סגור את כל היישומים לפני שאתה מוחק קבצים זמניים **או** חשודים. אולי תופתע לגלות שהיישום משתמש בקובץ שאתה מנסה למחוק. במקרה הטוב תצטרך לסגור את היישום **ו**להתחיל מחדש. במקרה הרע, מערכת ההפעלה יכולה להינעל **או** לקרוס.

תוכנות שירות לניקוי דיסקים

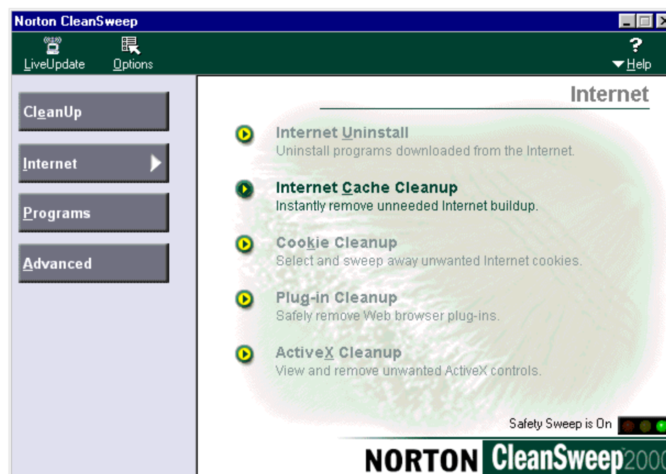
תוכניות שירות לניקוי דיסקים נועדו להסיר קבצים זמניים וקבצים חסרי ערך אחרים שיישומים רבים משאירים מאחוריהם, ולסייע בהסרת ההתקנה של תוכנות.

תוכנות כאלו מסייעות בהסרת קבצים זמניים מהסוג שדנו בהם. הן גם מבצעות מטלה חשובה בכך שהן נפטרות מקבצים חסרי ערך אחרים. שניים ממנקי הדיסקים הטובים יותר נידונים מטה.

Norton CleanSweep

Norton CleanSweep היא כנראה התוכנה היעילה ביותר מסוגה, ומספקת כמה תכונות שתוכנות אחרות אינן מספקות.

ההתמקדות העיקרית של Norton CleanSweep היא שחרור שטח דיסק, כפי שנרמז במסך התוכנה הראשי, המתואר בתרשים 6.5. CleanSweep גם מאתרת קבצים זמניים מסוגים רבים. בנוסף ניתן להתאים את התוכנה אישית לחפש או להימנע מסוגי קבצים מסוימים, לעבוד בתיקיות מוגדרות, ועוד.



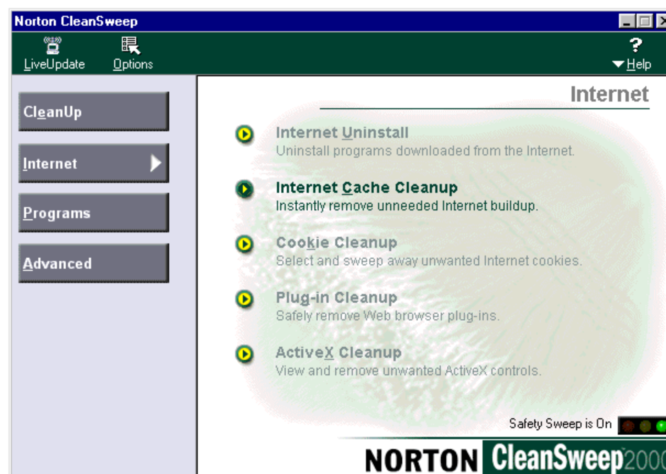
תרשים 6.5 Norton CleanSweep מסירה קבצים מיותרים.

Norton CleanSweep גם מטפלת בניקוי קבצי אינטרנט - נושא שנידון ביתר פירוט בפרק 9, וגם תקינות וניקוי ה-Registry. אם תרכוש את Norton System Works 2000, תוכנת CleanSweep כלולה בו.

Quarterdeck Remove-it

תוכנה זו תוארה בקצרה קודם. Remove-It גם מתמחה בהסרת תוכנות וקבצי אינטרנט מיותרים, אך עשויה גם להסיר קבצים זמניים רבים שנדרש להיפטר מהם. בין שאר הקבצים שהתוכנה מסירה נכללים תוכנות וקבצי INI מיותרים, קבצים כפולים, גופנים ומנהלי התקנים שאינם בשימוש, פקסים ישנים (חלקם עלולים לצרוך עשרות מגה-בייט), סמלים וקבוצות תוכנה שאין בהן תכולה או קישורים, קבצי תמונות ומולטימידיה שאינם בשימוש, ועוד.

עכשיו אתה יודע כיצד להיפטר מחומר מסוכן המונח בקבצים תמימים לכאורה, ולהסיר קבצים מחוקים וקבצים זמניים מיותרים מהדיסק לצמיתות. עתה נראה כיצד להוסיף הגנות חזקות לקבצים שאתה שומר, באמצעות הצפנת מידע.



תרשים 6.5 Norton CleanSweep מסירה קבצים מיותרים.

Norton CleanSweep גם מטפלת בניקוי קבצי אינטרנט - נושא שנידון ביתר פירוט בפרק 9, וגם תקינות וניקוי ה-Registry. אם תרכוש את Norton System Works 2000, תוכנת CleanSweep כלולה בו.

Quarterdeck Remove-it

תוכנה זו תוארה בקצרה קודם. Remove-It גם מתמחה בהסרת תוכנות וקבצי אינטרנט מיותרים, אך עשויה גם להסיר קבצים זמניים רבים שנדרש להיפטר מהם. בין שאר הקבצים שהתוכנה מסירה נכללים תוכנות וקבצי INI מיותרים, קבצים כפולים, גופנים ומנהלי התקנים שאינם בשימוש, פקסים ישנים (חלקם עלולים לצרוך עשרות מגה-בית), סמלים וקבוצות תוכנה שאין בהן תכולה או קישורים, קבצי תמונות ומולטימידיה שאינם בשימוש, ועוד.

עכשיו אתה יודע כיצד להיפטר מחומר מסוכן המונח בקבצים תמימים לכאורה, ולהסיר קבצים מחוקים וקבצים זמניים מיותרים מהדיסק לצמיתות. עתה נראה כיצד להוסיף הגנות חזקות לקבצים שאתה שומר, באמצעות הצפנת מידע.

פרק 7



הצפנת מידע

מה בפרק:

- ✓ מה היא הצפנה?
- ✓ כיצד מידע מוצפן?
- ✓ כיצד מידע מפוענח?
- ✓ דורות ופורמטים של מידע מוצפן
- ✓ יישום הצפנה
- ✓ תוכנות הצפנה

פרק זה מציג את מושג הצפנת קבצי מחשב, שהוא אמצעי למניעת אחרים מקריאה או מעיון בקבצים. נסביר מה היא בדיוק הצפנה, נסקור את סוגי הצפנת המידע שבשימוש, וכיצד לפענח מידע מוצפן.

לאחר מכן נדון ביישום הצפנה, ונסקור את תוכנות ההצפנה הטובות יותר הקיימות בשוק.

מה היא הצפנה?

הצפנה (Encryption) היא שינוי הודעה או מסמך באמצעות **קידוד (Encoding)** כך שתוכנו יהיה בלתי מזוהה (קידוד הוא הליך של המרת טקסט רגיל או מסמך ברור **לקוד (Code)**. קוד בהקשר זה הוא שיטת ייצוג נתונים באמצעות ערכת תווים מוגדרת מראש של אותיות, ספרות, סימנים מילים, ו/או אותות). מושג ההצפנה מתרחב גם לקבצי מחשב מכל סוג שהוא, ממסדי נתונים וגיליונות אלקטרוניים ועד תמונות וקבצי מעבד תמלילים.

הצד השולח מצפין והצד המקבל מפענח. המטרה בהצפנה היא למנוע שימוש במידע מאנשים שאין להם אמצעים ל**הסרת הקידוד (Decode)** או במילים אחרות, יכולת פענוח חוקית. רק בעלי אמצעים להסרת הקידוד יוכלו לקרוא את הקובץ.

הצפנה קיימת כבר לפחות 4000 שנה. אחד השימושים הידועים המוקדמים ביותר להצפנה היה ב- 1900 לפני הספירה לערך, כאשר פקיד מצרי החליף סימנים מיוחדים בהירוגליפים סטנדרטיים בכתובת. פחות מ- 500 שנה מאוחר יותר, הצפנה כבר שימשה במסמכים דתיים ונוסחאות, בנוסף לתכתובת ממשלתית.

הצורך באמצעי הצפנה יעילים עבור תקשורת צבאית, דיפלומטית, וממשלתית האיצה את התקדמות מדע ההצפנה. כיון שכיום קיימת תעבורת מידע כה גדולה בין מחשבים גם עסקים ויחידים מוצאים עניין בהצפנה.

דוגמה פשוטה של הצפנה

שורה בהודעת טקסט מוצפנת שנוצרה על ידי החלפה פשוטה של תווים עשויה להיראות כך: 1zdvrqwkhjuduubnroo.

על פניו 1zdvrqwkhjuduubnroo נראה כטקסט חסר משמעות. אולם, אם ידעת שכל אות הוזזה שלוש אותיות קדימה באלף-בית (a הפכה ל- d, m הפכה ל-p, y הפכה ל-b - כיון שצריך לחזור להתחלה כדי לעבור את z - וכן הלאה), יכולת לפענח בקלות את 1zdvrqwkhjuduubnroo- ולראות שמשמעותו היא iwasonthegrassyknoll. הוסף רווחים בין מילים ותקבל את המשפט הברור: I was on the grassy knoll (הייתי על התל המכוסה דשא).

זו היא דוגמה בסיסית ביותר של הצפנה. הצפנה באמצעות מחשב מבוססת על תבניות מורכבות בהרבה - ותבניות בתוך תבניות.

כיצד נתונים מוצפנים

באופן מעשי, הצפנה היא לרוב הליך **החלפה (Substitution)**. ערך חליפי (הידוע גם כ**אסימון [Token]**, או כאשר מדובר בתו בודד **תו אסימון [Token Character]**) מוקצה במקום חלקים מוגדרים של הודעה או נתונים, לעיתים קרובות ברמת התו. לדוגמה, האות **r** עשויה להתחלף באות **m**, או הספרה **9** תוחלף בספרה **3** או בספרה **0**. כמובן שלא משתמשים רק באותיות וספרות; ניתן גם להשתמש ב- **?**, **XXX**, # או אפילו רווח יכול לשמש כתחליף או תו אסימון. או **bb** עשוי להיות מוחלף ב- **2b**. תוך שילוב רעיונות אלו ניתן לקדד את המילה **Three (שלוש)** ל- **pkm2f** (מתוך הנחה ש-**p** מחליף את **t**, **k** מחליף את **h**, **m** מחליף את **r**, ו- **f** מחליף את **e**).

הדוגמאות שלעיל מתייחסות לקבצי טקסט. אולם, ניתן לקדד נתוני 8 סיביות או בינאריים בצורה דומה באמצעות החלפות. ניתן להחליף תווי 8 סיביות אחרים בתווים המקוריים במסמך, או להחליף תווי 7 ו- 8 סיביות בערבוביה. או, ניתן להשתמש רק בתווי 7 סיביות לצורך החלפה (למעשה, זו היא השיטה בה משודרים קבצי דואר אלקטרוני רבים; באמצעות קידוד, הקובץ מוסב מתווי 8 סיביות לתווי 7 סיביות, הניתנים לשידור בקלות בערוצי מודם רגילים).

בנוסף, כיון שניתן ליצור החלפה של **rrrrwww** ב- **4r3w**, לעיתים קרובות נתונים מוצפנים גם נדחסים.

קידוד נתונים מיוחד לשידור קבצי 8 סיביות

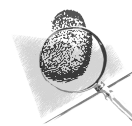
תעבורת נתונים רגילה עם מודמים וקווי טלפון אינה משתמשת בתווים בפורמט 8 סיביות כנתונים. נתונים המשודרים באמצעות מודם חייבים להיות בפורמט 7 סיביות, כיון שתווים רבים בני 8 סיביות המופיעים בקובץ בינארי (גרפיקה, לדוגמה) משמשים כתווי בקרה ואותות ליציאות טוריות, מודמים ותוכנת שידור.

לכן, כאשר קובץ בינארי מוסב כך שניתן לטפל בו כקובץ ASCII בן 7 סיביות, תווים בני 8 סיביות מוחלפים בתווים בני 7 סיביות. תבניות ההחלפה קבועות מראש ומבוססות על פורמט ידוע (UUENCODE, MIME, או אחר). כך, אין כל בעיה בפענוח הקידוד בצד שמקבל את שידור הנתונים.

קידוד כזה נראה כתווים אקראיים, כמו בדוגמה מטה:

foXwAAAQMjpgsAAAEDAMsiJK9Ah6VAXVfob34chAeLeWx

לתוכנה בצד המקבל כמובן, **יש** את **המפתח** (קוד התרגום) להסבת הקובץ בחזרה לפורמט המקורי שלו, של נתונים בינאריים.



למידע נוסף על קבצי נתונים, 7 ו- 8 סיביות, bytes, ונושאי מחשב קשורים לכך, ראה פרק 6.

לעיתים, אך לא תמיד, הליך הקידוד מחליף כל תו. בנוסף, ההחלפה לא נעשית תמיד על בסיס תו מול תו. תו אחד עשוי לייצג מילה שלמה או קבוצת bytes. או, רק כדי לסבך את הדברים עוד יותר, מילה (או קבוצת bytes) יכולים לייצג תו אחד או ספרה בודדת.

רוב תוכנות ההצפנה יוצרות מגוון תבניות החלפה כך שלא ניתן לזהות את התבנית ולהשתמש בה ככלי פענות. סוג ההחלפה המתבצע (תו אחד במקום רבים, רבים במקום אחד, תבניות חוזרות או לא חוזרות) ו/או תבניות ההחלפה, מכונה קוד, או **chipher (קידוד).**

כיצד נתונים מפוענחים

פענוח (Deciphering ,Unencryption, Decryption), הוא הליך של שחזור נתונים מהודעה מוצפנת בהתבסס על קוד ידוע, או צופן. הקוד מפוענח באמצעות רשימה, טבלה או מפתח.

בתיאוריה, לא ניתן לקרוא מידע מוצפן ללא **מפתח** שישמש כמדריך לכל ההחלפות שבוצעו בעת הקידוד. אולם, די קל לפענח תבנית פשוטה ואחידה של החלפת תווים (לדוגמה, אם **m** תמיד מחליפה את **r** וכך הלאה, או ההחלפה המוסטת שתוארה בטקסט, קודם).

מפתח יכול לקבל צורות רבות - טבלה המראה את ההחלפות תו-מול-תו, או מילה-מול-מילה, או מערכת החלפות מתוחכמת יותר (טכניקות ההצפנה המקובלות ביותר כיום משתמשות באלגוריתמים מתמטיים מתוחכמים).

אם נניח שסכמה או תבנית ההצפנה הם מסובכים מדי לפענוח או "פיצוח", הדרך היחידה לקרוא את ההודעה המוצפנת היא באמצעות טבלה של החלפות שבוצעו. או, במקרה של קובץ נתונים שהוצפן על ידי מחשב, עליך להשתמש ב**תוכנת פענוח** ומפתח לנתונים המוצפנים (לרוב, תוכנת ההצפנה יכולה לתפקד גם כתוכנת הפענוח).

ככלל, פענוח קבצים שהוצפנו על ידי מחשב כרוכה בסיסמה להרצת תוכנת הפענוח, או להרצת ארכיב נפרש-עצמית המכיל את הקובץ המוצפן. האדם שמצפין את הנתונים מגדיר את הסיסמה.

צורות ופורמטים של נתונים מוצפנים

קובץ נתונים מוצפן עשוי להיות בצורה של תווים מוחלפים (או תווים בודדים המוחלפים בקבוצות תווים), כפי שנידון קודם. קובץ טקסט בצורה זו יהיה מורכב ממחרוזות תווים חסרי משמעות. קובץ נתונים בינארי יכיל מחרוזות של תווי 7 ו- 8 סיביות ששום יישום לא יוכל לעבוד עמם.

בנוסף, קובץ נתונים מוצפן יכול להיות בצורת **ארכיב פרישה-עצמית** - תוכנה עצמאית היוצרת גירסה מפוענחת של הנתונים המוצפנים שהיא מכילה (ראה פרק 4 למידע נוסף על ארכיבים). בשני המקרים, לרוב נדרשת סיסמה להגיע לנתונים המוצפנים.

ישנן מספר גישות להצפנת דואר אלקטרוני. ככלל, ככל שההגנה חזקה יותר, כך תוכנית היישום שלה מורכבת יותר.

הצפנה ידנית של הודעות

הגישה הפשוטה ביותר היא לתרגם הודעה בצורה ידנית לקוד שהנמען מבין. זה יכול להיות ערכת מילות קוד, צופן החלפת תווים או טבלת החלפות אקראיות שיצרו משתמשי הצופן.

הצופן עשוי להתבסס על נוסחה - אולי הערך המספרי של כל אות באלף-בית (1 עד 22), מוכפל ב- 2, והוספת 9 (במקרה זה "cab" ייהפך ל- "13, 11, 15"). לעיתים קרובות, ההצפנה תלויה בנוסחה מתמטית, או **אלגוריתם (Algoritm)**, הנידון בסעיפים הבאים והוא מורכב בהרבה מדוגמה זו.

הצפנה אוטומטית

גישה נוספת להצפנת דואר אלקטרוני היא שימוש בתוכנה מיוחדת המערבלת את הנתונים על ידי הקצאת ערך מספרי לכל תו (באנגלית - Hashing Data). תוכנה דומה בצד השני יכולה לפענח את הנתונים, בתנאי שהנמען משתמש בסיסמה המוגדרת על ידי האדם שיצר את ההודעה המקודדת. זה הבסיס למספר תוכנות הצפנה וזה לרוב קל יותר מאשר יצירת צופן עצמאי בצורה ידנית.

קבצי ארכיב בפרישה-עצמית

אפשרות מתקדמת יותר היא הצפנת קובץ ודחיסה שלו לתוכנה, שבעת הרצתה, מפענחת אותו. התוכנה החדשה שנוצרה, היא למעשה, ארכיב בפרישה-עצמית.

תוכנת הפרישה נוצרת על ידי תוכנה מיוחדת שקודם מצפינה את הנתונים, ואז מאחסנת אותם בארכיב לפרישה-עצמית. הנמען צריך רק להריץ את הארכיב בפרישה-עצמית, לאחר שנתן את הסיסמה המתאימה. בשלב זה הקובץ מפוענח. ארכיב פרישה-עצמית יוצר קובץ שלתוכו הוא קורא את הנתונים המוצפנים והופכם לטקסט קריא. תוכנת Norton Secret Stuff, הנידונה בהמשך, מתאימה ביותר למטרה זו.

הצפנה באמצעות מפתח ציבורי ופרטי

קיימת אבטחת הגנה באמצעות תקן הנקרא **SSL** (אלו הן ראשי תיבות של **S**ecure **S**ockets **L**ayer). אבטחה בתקן **SSL** עושה שימוש בשני מפתחות לצורך יצירת האבטחה:

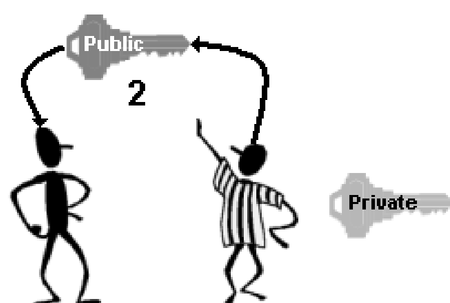
1. **מפתח ציבורי** (Public Key),
2. **מפתח פרטי** (Private Key),

לרוב אנו מכירים מנעול אחד ומפתח אחד המתאים לו. כמובן שנוכל לשכפל את המפתח היחיד שלנו ואז כל מי שבידו המפתח המתאים לאותו מנעול יוכל להיכנס. הבעיה במפתח בודד היא שאנו לא יודעים האם המפתח נמצא בידיים הנכונות, והרי כל מי שבידו מפתח מתאים יוכל להיכנס.

שיטת שני המפתחות פועלת כך: נניח שישנם שני חברים, דני ומיקי. דני רוצה להעביר מסר למיקי, אבל רוצה להיות בטוח שרק מיקי יוכל לקרוא אותו ולא מישהו אחר. מה עושים?

1. מיקי מייצר שני מפתחות שונים: Public key ו- Private key שרק באמצעות שניהם ניתן לקרוא את המסר.





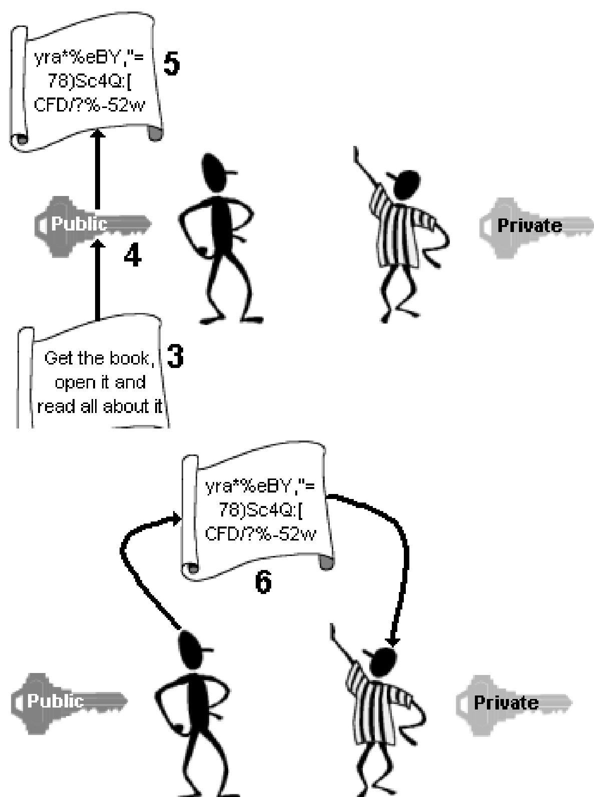
2. מיקי שומר מפתח אחד (Private key) אצלו ואת המפתח השני (Public key) הוא שולח לדני.

3. דני כותב את המסר במעבד תמלילים.

4. דני מצפין את המסמך בעזרת המפתח הציבורי שקיבל ממיקי.

5. דני מקבל מסמך מוצפן.

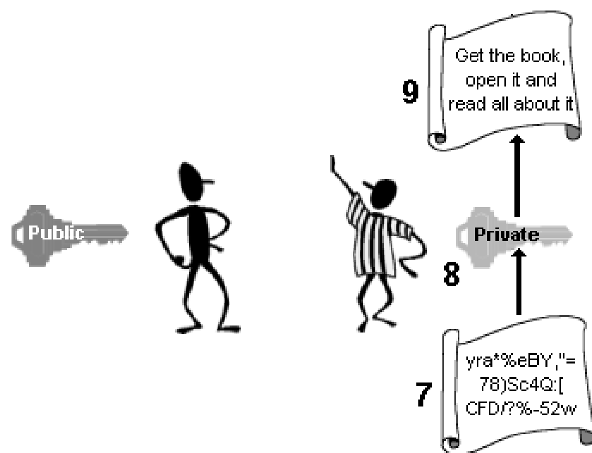
6. דני שולח את המסמך למיקי.



7. מיקי לוקח את המסמך המוצפן.

8. מיקי מפענח את המסמך בעזרת המפתח הפרטי שבידיו.

9. מיקי קורא את מה שכתב לו דני.



שיטת המפתח הציבורי והמפתח הפרטי מספקת סודיות, על ידי כך שהיא מבטיחה שרק הנמען הרצוי יוכל לפענח ולצפות בתוכן הנתונים. כאשר יש צורך להעביר נתונים באופן מאובטח, משיג השולח (דני) את המפתח הציבורי של הנמען (מיקי). השולח (דני) משתמש במפתח הציבורי של הנמען כדי להצפין את הנתונים, ואז שולח אותם. כאשר הנמען (מיקי) מקבל את הנתונים המוצפנים, הוא משתמש במפתח הפרטי שלו כדי לפענח אותם. ההצפנה מאובטחת רק אם השולח משתמש במפתח הציבורי של הנמען לצורך הצפנה.

המפתחות הם כל כך מורכבים ומסובכים, שצריך מחשב כמו זה הנמצא ב-NASA, סוכנות החלל האמריקאית, שיעבוד כמה שנים כדי לפצחם.

יישומי הצפנה

הצפנה היא אמצעי מצוין להגנת מידע מכל סוג. קבצי טקסט, מידע בינארי וקבצי תוכנה, ואף גרפיקה ניתנים להצפנה, לאחסון או שידור.

השימוש העיקרי של הצפנת מידע הוא הגנת מידע הנמצא בקבצים הנגישים לאחרים. בהתאם לרמת הידע שלהם בתחום המחשבים, נדרש להצפין קבצים על הדיסק הקשיח, אף אם הקבצים מוגני-סיסמה ו/או בלתי נראים.

אם יש חשש שהדואר האלקטרוני שלך או קבצים שאתה שולח באינטרנט יפלו לידיים זרות, רצוי גם להצפין את המידע שנמצא בהם.

הצפנת קבצים מאוחסנים

אם ברצונך למנוע את הטרחה הכרוכה בהעתקת קבצים הלוך וחזור, או הפיכת קבצים ותיקיות לבלתי נראים, תמצא שהצפנת קבצים היא דרך מעשית להגנה על המידע תוך השארתו על הדיסק הקשיח. אף אם אתה מאחסן קבצים רגישים על דיסקט מוחבא, שקול הצפנת קבצים אלה במקרה שמישהו ימצא את הדיסקט.

הצפנה היא גם שיטה טובה להגנת קבצים על דיסקים קשיחים של מחשבים ניידים. כיון שמחשבים ניידים נגישים לאנשים רבים, המידע עליהם פגיע במיוחד. אם אתה מחזיק קבצים רגישים על מחשב נייד - שלך ו/או של לקוחות או המעסיק - רצוי להגן על קבצים אלה.

הצפנת דואר אלקטרוני

משתמשי מחשבים רבים מוטרדים מכך שהדואר האלקטרוני שלהם עלול להיקרא על ידי אנשים אחרים. חוק פרטיות התקשורת האלקטרונית אוסר על קליטה וקריאת דואר אלקטרוני פרטי. כיון שכך, האם באמת צריך לשקול הצפנת דואר אלקטרוני? התשובה היא "כן", כיון שחוק כשלעצמו אינו מונע את המעשה עליו הוא אוסר. בנוסף, מנהלי מערכות או אחרים בארגון פטורים מחוק זה בנוגע לדואר אלקטרוני של עובד. כמו כן, דואר אלקטרוני עלול להיות בעל כתובת שגויה או להגיע ליעד לא מתוכנן מסיבה כלשהי.

הצפנה מגינה על הודעות דואר אלקטרוני כנגד איומים כאלה. כיון שרק אתה והאנשים אליהם אתה שולח דואר אלקטרוני מוצפן יכולים לקרוא אותו, אין סכנה של פריצת המידע.

הצפנת שידור נתונים

אם אתה מתכוון לשלוח קבצי נתונים רגישים לאחרים, או לאחסן קבצים באחסון מקוון (כפי שנידון בפרק 4), יש להניח שתרצה להצפין קבצים אלה. זה נכון גם לגבי קבצים לאחסון מקוון.



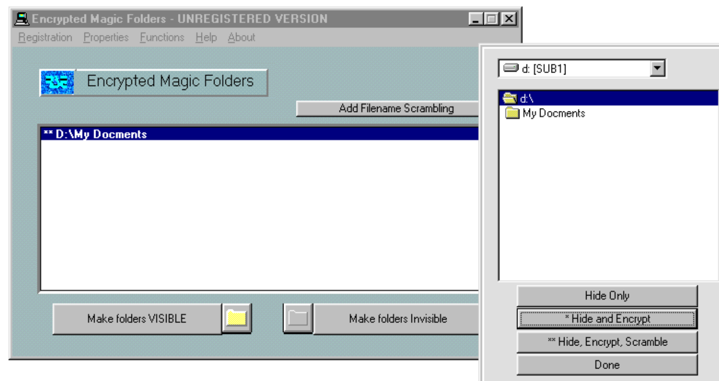
אם תצפין דואר אלקטרוני או קבצים שאתה שולח למישהו אחר, עליך לתת לנמען את הסיסמה הנדרשת לצפייה בנתונים האמורים. לא כדאי לשלוח סיסמאות באמצעות דואר אלקטרוני. במקום, תן לנמענים שלך את הסיסמאות באופן אישי או דרך הטלפון.

תוכנות הצפנה

תוכנות הצפנה אינן בדיוק קטגוריית התוכנה הפופולרית ביותר, אך עדיין יש כמה תוכנות מסחריות ושיתופיות טובות היכולות לטפל כמעט בכל צורכי ההצפנה. כמה מתוכנות אלו שנדון בהן כאן הן חלק מחבילת תוכנה כוללת ואלו ניתנות לרכישה בנפרד.

Encrypted Magic Folders (EMF)

Encrypted Magic Folders (EMF) מאפשרת הצפנת קבצים בתיקיות. בנוסף, ל-EMF יש אפשרות להפוך קבצים ותיקיות אלה לבלתי נראות. כמתואר בתרשים 7.1, ל-EMF יש ממשק משתמש פשוט ביותר. לחץ על תיקיות שאתה רוצה להצפין, הכנס סיסמה, והמערכת עובדת.



תרשים 7.1 EMF מצפינה קבצים והופכת קבצים ותיקיות לבלתי נראים.

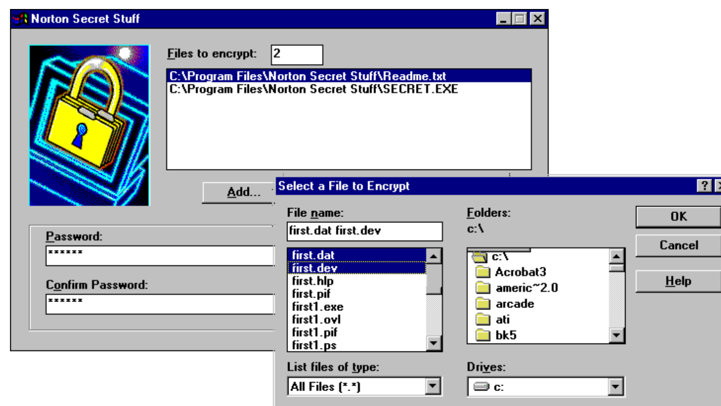
כאשר אתה רוצה להשתמש בקבצים המוצפנים, הפוך את ההליך. עליך להכניס את הסיסמה פעם אחת בלבד לקבלת גישה מלאה לכל קבציך.

Encrypted Magic Folders (EMF) היא תוכנה שיתופית (Shareware).

Norton Secret Stuff (NSS)

Norton Secret Stuff (NSS) היא תוכנה הכלולה בתוכנות Norton System Works של Symantec. זו היא תוכנה מסחרית.

NSS יוצרת ארכיבים בפרישה-עצמית. ממשק המשתמש של NSS, המתואר בתרשים 7.2, הוא פשוט וישיר.



תרשים 7.2 ממשק המשתמש של Norton Secret Stuff (NSS)

פשוט בחר את הקבצים שברצונך להצפין (תוכל לכלול עד 2000 קבצים בארכיב לפרישה-עצמית), הכנס סיסמה, ולחץ על לחצן Encrypt (הצפן). תוצג שאלה לשם הקובץ, ו-NSS תצפין ותכווץ את הקבצים הנבחרים ותיצור קובץ הפעלה לפרישה-עצמית.

לפענוח קבצים, לחץ פעמיים על הקובץ לפרישה-עצמית מסייר Windows (או בחר אותו בתפריט **התחלה**, ולחץ על **הפעלה**. NSS תנחה אותך לקבלת סיסמה. לאחר שהסיסמה הנכונה סופקה, NSS תשחזר את הקבצים לצורתם המקורית. כנמען של הודעה המוצפנת באמצעות NSS, אינך צריך את תוכנת Norton Secret Stuff (NSS) לפענוח הקבצים; כל שנדרש הוא הקובץ לפרישה-עצמית (הקובץ המוצפן) שנשלח אליך וסיסמה נכונה. לא נדרשת תוכנה נוספת. זאת כיון שהארכיב לפרישה-עצמית **הוא** התוכנה.

דבר זה נכון גם לגבי קבצים המוצפנים על הדיסק הקשיח. תוכל, אם תרצה, להסיר את NSS מהמערכת ועדיין תוכל לפענח קבצים, בתנאי שיש לך את הסיסמה המתאימה.

בסך הכל, זו תוכנת ההצפנה הפשוטה ביותר בשוק, אך היא יעילה מאוד בהגנה על קבצים שאתה רוצה לשדר למישהו אחר, ועל קבצים רגישים שעליך לשמור על הדיסק הקשיח. תוכנה זו מאוד מומלצת.

למידע נוסף אודות NSS ותוכנות שירות אחרות של Norton, ראה באתר:

http://www.symantec.com

Pretty Good Privacy (PGP)

השם מעלה אולי נשמע היתולי, אך זו כנראה תוכנת ההצפנה באמצעות מפתח ציבורי/פרטי הטובה ביותר בשוק. Pretty Good Privacy, או בשמה המקוצר PGP, היא גם התוכנה הנפוצה ביותר מסוגה.

בנוסף ליצירת מפתחות ציבוריים ופרטיים, PGP כמובן גם מצפינה הודעות באמצעות מפתחות ציבוריים ומפענחת הודעות באמצעות המפתח הפרטי של המשתמש. כמו כן PGP גם מספקת אימות הודעות באמצעות **חתימות דיגיטלית**, הנוצרות אף הן על ידי תוכנת PGP.

חתימה דיגיטלית היא מחרוזת תווים ייחודית לזיהוי, המשמשת כאמצעי לאימות דואר אלקטרוני. בשלב הראשון, כל תו בהודעה מקבל ערך מספרי. אז, אלגוריתם מתמטי מסובך מחולל מחרוזת ערכים מספריים שכמעט לא ניתן לשכפל או לפצח. ערכים אלה מתווספים לסוף ההודעה כחתימה דיגיטלית ומאוחסנים על ידי המערכת שיצרה אותם להשוואה עתידית כנדרש.

קבצי מפתחות ציבוריים וחתימות דיגיטליות הנוצרים באמצעות PGP הם קבצי טקסט הדומים לגוש התווים שבתרשים 7.3.


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.2

foXwAAAQMjpgsAAAEDAMsiJK9Ah6VAXVfobv34chAeLeWxl
23OLhBEskOAc01nwbWugMgSs39dfda996eWd5IFNhbGVzIDxzYcrn0hBEskBzeh
f3QJfoXou39Y29VfobvtPg==
=wPgw
-----END PGP PUBLIC KEY BLOCK-----
```

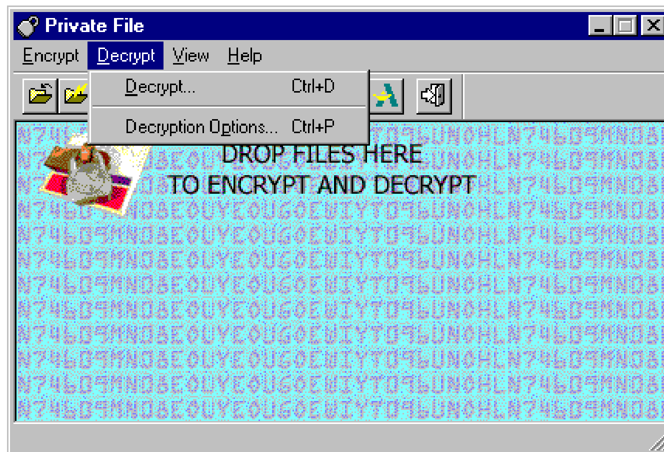

תרשים 7.3 מפתח ציבורי שנוצר על ידי Pretty Good Privacy

באמצעות PGP תוכל ליצור מפתח ציבורי ולהפיצו לחבריך, עמיתיך, ואחרים. אמצעי אחד להפצת המפתח הציבורי שלך הוא להוסיפו אחרי ה"חתימה" שלך בסוף כל הודעה (תוכל לעשות זאת ביעילות מירבית על ידי הוספתו לקובץ sigfile - הידוע גם כ-signature file - שהוא גוש טקסט המוגדר על ידי המשתמש שתוכנות דואר אלקטרוני רבות ממקמות באופן אוטומטי בסופן של ההודעות היוצאות).

PGP נכתבה על ידי Phillip Zimmerman ומופצת חינם (Freeware).

Private File 2

Private File היא תוכנה מסחרית המספקת הצפנה חזקה וממשקי משתמש שונים. כמתואר בתרשים 7.4, ניתן להשתמש בממשק גרור ושחרר (Drag & Drop) להניח קבצים להצפנה או פענוח בתיבה על שולחן העבודה. לחליפין, ניתן להשתמש בבחירה מתפריט להצפין ולפענח קבצים נבחרים.



תרשים 7.4 ממשק גרור ושחרר של Private File.

הקבצים מוצפנים ומפוענחים באותה תוכנה. נדרשת סיסמה לשתי הפעולות (תוכל להכניס סיסמה פרי המצאתך, או Private File תחולל סיסמה אקראית), וקבצים נדחסים בעודם מוצפנים. כאפשרות, ניתן למחוק את הקובץ המקורי לאחר הצפנתו (הליך המחיקה מיישם טכניקת מחיקה בת שלושה מעברים המוגדרת על ידי ממשלת ארה״ב. לפרטים על אופן פעולתה, ראה כתובת: http://www.aladdinsys.com/privatefile/protect.html).

ניתן גם לשלב את Private File עם תוכנת דואר אלקטרוני להצמדת קבצים מוצפנים להודעות אוטומטית.

יש לציין ש-Private File פועלת היטב במערכות Mac ו-Windows - כלומר ניתן לשתף קבצים מוצפנים בין מחשב Mac למחשב Windows, בתנאי ששניהם מריצים את Private File ביחד.

Private File היא תוכנה מסחרית. למידע נוסף ראה Aladdin Systems, בכתובת:

http:\\www.aladdinsys.com

SecurePC 2

SecurePC היא תוכנה מסחרית של חברת RSA Data Security. SecurePC מיועדת להיות תוכנה עצמאית להצפנת נתונים על הדיסק הקשיח של מחשב בודד או ברשת. ברמת קבצים ותיקיות.

ניתן להצפין קבצים לפענוח מאוחר יותר באמצעות SecurePC, או ניתן להשתמש בתוכנה ליצירת ארכיבים לפרישה-עצמית.

בנוסף להגנת ההצפנה, SecurePC מציעה גם אפשרות הגנה עם סיסמת אתחול - כלומר, צריכה להיות סיסמה כדי להתחיל את Windows לאחר החלת אפשרות זו.

למידע נוסף על SecurePC, הגנת מידע ותקנים, ופעילות חברות שונות בנושא אבטחה באינטרנט, גש לאתר RSA Data Security: http://www.rsasecurity.com. ארגון זה אחראי לתכנון ויישום רוב תקני האבטחה המשמשים באינטרנט.

נחזור לנושא ההצפנה בפרק 10. בפרק 8 נדון בנושא וירוסים של מחשבים וכיצד להגן על המערכת שלך מפניהם.

פרק 8



הגנה מפני וירוסים

מה בפרק:

- ✓ *מה הוא וירוס מחשב?*
- ✓ *היכן התחילו הווירוסים ומדוע?*
- ✓ *איזה סוגי וירוסים קיימים?*
- ✓ *מה עושות תוכנות וירוס?*
- ✓ *וירוסים של יישומים בדפדפני אינטרנט*
- ✓ *תוכנות נגד וירוסים*
- ✓ *מתיחות ותראיות וירוסים*

פרק זה בוחן מה הוא בדיוק וירוס מחשב, מה באפשרותו לעשות, ומדוע וירוסים קיימים. נוסף לכך, תלמד כיצד וירוסים וסוסים טרויאניים יכולים לחדור למחשב.

לאחר שנבין וירוסי מחשב, נציג אמצעי הגנה נגד תוכנות ויראליות אלו המגיעות באופן מקוון ולא מקוון. נבחן נקיטת אמצעי זהירות, ומה קיים בתחום תוכנות האנטי-וירוס. לבסוף, נאמר מספר מילים על מתיחות ותרמיות וירוסים.

מה הוא וירוס מחשב?

במובן הפשוט ביותר, וירוסי מחשב הן תוכנות או פקודות מאקרו הפועלות - לעיתים קרובות פעולה הרסנית - בצורה שאינך מצפה או רוצה שיפעלו. הם יכולים להציג הודעות פוליטיות או מעליבות על המסך, למחוק קבצים מהדיסק הקשיח, או למחוק את מערכת ההפעלה של המחשב. כמה תוכנות וירוס פועלות על בסיס השהיית זמן, כך שהמשתמש בהם מעביר אותם הלאה לפני שהבחין בפעולתם. רבות מהן מקננות בחשאי, תוך שינוי איטי של קבצים נבחרים, ואז יום אחד - **בום!** - המערכת שלך אינה עובדת. מגוון תוכנות הווירוס הוא אינסופי, אך התוצאה הסופית זהה: הפרעה או הרס פעולת המחשב.

למעשה, השם **וירוס** מתאים ביותר. וירוסים של מחשבים מחקים וירוסים ביולוגיים בדרכים רבות. בדיוק כמו שוירוס שפעת מתחבר למארח אנושי, וירוסים של מחשבים מצמידים את עצמם לתוכנות וקבצים. וכמו וירוס השפעת, וירוסים של מחשבים מדבקים, וחלקם משתמשים במשאבי מערכת מחשב מארחת להתרבות ולשכפל את עצמם.

רוב הווירוסים מוסווים כתוכנות ציבוריות או שיתופיות, אך יש גם וירוסים שהופצו בתוך העתקי תוכנות חוקיות ולא חוקיות של תוכנות מסחריות. אלה החומקים לתוך המערכת כשהם מחופשים לתוכנות חוקיות נקראות לעיתים תוכנות **סוס טרויאני**.

מקור השם סוס טרויאני

השם **סוס טרויאני** מתייחס לתרגיל שאודיסאוס והצבא היווני עשו לתושבי העיר המבוצרת טרויה בתחילת המאה ה- 12 לפני הספירה. היוונים הצליחו להגניב חיילים לתוך העיר בתוך מה שנראה כסוס עץ ענקי. לפי האגדה, הטרויאנים האמינו שהסוס הוא מתנה מהאלים שלהם והכניסו אותו לתוך עירם המבוצרת. מאוחר באותו לילה, החיילים שהתחבאו בסוס יצאו החוצה ופתחו את השערים לצבא היווני - וטרויה הפכה להיסטוריה.

שם זה מתאים כיון שתוכנות סוס טרויאני נראות מפתות - אולי משחק טוב, תוכנת האקרים (Hacking), או אף העתק לא חוקי של תוכנה מסחרית יקרה. מתברר כי לא כך הדבר לאחר הרצת התוכנה, כיון שהיא גונבת מידע, הורסת קבצים, או מזיקה למערכת בדרך אחרת.

היכן מקור הווירוסים?

וירוסי המחשב המקוריים היו כנראה הלצה בין מתכנתי מערכות מחשב גדולות ומערכות מיני עוד בשנות ה- 60'. כאשר הופיעו המחשבים האישיים הראשונים, היה זה אך טבעי, שהאנשים המוכשרים בעלי הנטייה הטכנית שנהגו אז לרכוש אותם, יחשבו על תוכנות חכמות ובלתי צפויות, ועל הלצות נוספות.

פעילות זו היתה בלתי מזיקה בתחילה; אך ככל שרבו האנשים העוסקים במחשבים אישיים, וכלי התוכנה למתכנתים ולאנשים רגילים נעשו חזקים ומתוחכמים יותר, הדברים החלו לגלוש מעבר להלצות ולמעשי קונדס.

עד לאמצע שנות ה- 80' וירוסי מחשב היו די נדירים (יש להניח שרוב האנשים בעלי יכולת כתיבת וירוסים אז, היו עסוקים בפריצה לתוכנות מוגנות-העתקה). עד אז, אמצעי ההפצה של תוכנות וירוס לא היו כמעט בנמצא. ככל שהשיתוף בתוכנות התרבה - באמצעות דיסקטים או מודם - כך גברו מקרי ההתקפה בזדון של וירוסים על מחשבים.

באותה תקופה הופיעו גם מספר סוגים של וירוסים "חיים" או כאלה המשכפלים את עצמם, שפלשו למחשבים גדולים ומחשבי-מיני, בנוסף לרשתות מחשבים מתמחות של חברות ציבוריות ופרטיות, והפריעו לדואר אלקטרוני ופעולות אחרות (בין אלה היה וירוס רשת IBM המפורסם, שהיה מסוגל לשכפל את עצמו ולנוע דרך הרשתות, כמעט כאילו היה יוצר חי המנחה את עצמו).

בעוד וירוסים של מחשבים החלו לככב בעיתונות בסוף שנות ה- 80', הופיעו עוד וירוסים, במתכונת של חקייני-פשע. חלקם היו במתכונת די יצירתית ונועזת. לפחות וירוס אחד הוכרז מראש על ידי יוצרו שהודיע שהוא רק יציג הודעה בקשר לשלום עולמי בתאריך מסוים. היו גם כמה וירוסים ערמומיים במיוחד שהתחפשו כתוכנות אנטי-וירוס.

היום משערים, שלכל הפחות שתיים עד שלוש תוכנות וירוס חדשות מופיעות מדי יום.

מדוע וירוסים קיימים?

אנשים יוצרים וירוסי מחשב ממיגוון סיבות. הסיבות כוללות:

- נקמה כנגד מערכת מסוימת או קבוצת מחשבים
- הצורך בהישג מרשים (אפילו אם הוא אנונימי)
- מהתלה
- הצהרות פוליטיות
- ניסוי ("לראות אם ניתן לעשות זאת")

העיתונות הצהובה נתנה גוון גאוני לחלק מיוצרי הווירוסים. בו בזמן, מקורות מדיה אחרים טענו שאחדים מיוצרי הווירוס הם האקרים (Hackers) לא שפויים, חסרי הצלחה בחייהם הפרטיים והם פשוט מיישמים צורך מושרש עמוק לשלוט על דברים.

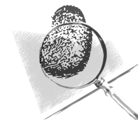
הסיבה שמתכנתים יוצרים וירוסים או תוכנות סוס טרויאני, היא חסרת משמעות אם נדבקת בווירוס. לכן, יש לנקוט כל אמצעי זהירות נגדם.

איזה סוגי וירוס קיימים?

הווירוסים באים במיגוון צורות. חלקם מופעלים רק בתאריכים מסוימים. אחרים פועלים רק בעת הפעלת תוכנה מסוימת, או כאשר תוכנה כלשהי פונה למערכת ההפעלה. ויש וירוסים המופעלים מייד עם אתחול המחשב.

מה הם עושים?

וירוסים עלולים לבצע מיגוון רב של פעולות: הם הורסים נתונים, גונבים מידע, חוסמים או מונעים את הפעלת המחשב, או עושים דברים מוזרים כמו אתחול מחדש של המחשב, או הבהוב המסך. חלקם רק "מציקים" לך על ידי הפרעה לפעולת המחשב.



דבר אחד שווירוסי מחשב אינם עושים זה להזיק לחומרה. כמו כן הם אינם גורמים נזק פיסי לדיסק. נתונים על דיסק עלולים להינזק או להיהרס, והתקנים כמו המסך והמדפסת עשויים לפעול בדרך לא צפויה; אך לא נעשה להם נזק פיסי.

המשמידים

סוג הווירוס הידוע ביותר הוא זה שפועל ללא ליאות בהשמדת נתונים, תוך מחיקת כל הקבצים בתיקיה או בדיסק קשיח, או הורס או מוחק קבצי מערכת הפעלה ברגע שאתה מריץ תוכנה שאליה הם מחוברים. אחרים יוצרים קבצי זבל הולכים וגדלים בניסיון לסתום (או "לפוצץ") את הדיסק. יש שמבצעים שינוי קל במספר תוכנות או קבצי מערכת הפעלה על הדיסק הקשיח, אולי תוך שכפול או העתקת עצמם בתוך התוכנות האלו, עד שהמטרה המסוימת הושגה - בנקודה זו אף תוכנה אינה עובדת יותר.

וירוסים המשכפלים-את-עצמם

וירוסים המשכפלים-את-עצמם מזיקים באופן מיוחד, כיון שהם יכולים לשרוץ בכל אחד ממאות הקבצים במחשב. גם אם תיפטר ממופע אחד או שניים שלהם, יש להניח שישנם עוד. חלקם ימתינו עד שיהיו מספר קבצים נגועים על הדיסק הקשיח כדי להבטיח קריסת מערכת ההפעלה, וגם לתת לך הזדמנות לשתף קובץ נגוע אחד או יותר. מטרתם היחידה בשורה התחתונה היא ריבוי והפצה.

גניבת מידע

חלק מתוכנות הסוס הטרויאני נכתבו מפורשות לגניבת זיהויי משתמש (User ID) וסיסמאות גישה לשירותים מקוונים או ספקי גישה לאינטרנט (ISP). הגולשים הם מטרה נפוצה לתוכנות אלו, הרצות ברקע בעודך מקוון, ושולחות את הסיסמה והזיהוי שלך באמצעות דואר אלקטרוני או בדרך אחרת, אל האדם שכתב את התוכנה.

כמה תוכנות מאקרו וסוסים טרויאניים מעניינים שימשו אף הם לגניבת מידע - בעיקר לצורך שכפול עצמי. אחד מווירוסים אלה תקף את תוכנת הדואר האלקטרוני Outlook Express, והשתמש ברשומות ספר הכתובות כדי למען העתקים של עצמו לאחרים, כך הוא הדביק את המחשבים וחזר שוב ושוב על התהליך. בסופו של דבר, הוא הגיע לעשרות אלפי מחשבים.

אובססיית שליטה

הווירוסים החמקניים ביותר יכולים להשתלט על המחשב, להריץ ולכבות תוכנה כאילו באקראי. יש וירוסים המתוכנתים לעשות כך פשוט לשם השעשוע, ויש אחרים המריצים תוכנות בזמנים קבועים כדי לגנוב מידע.

ישנם גם סוסים טרויאניים העובדים ברקע כדי לשלוח מידע גנוב באמצעות דואר אלקטרוני, כמתואר קודם לכן, ולשדוד מידע פיננסי מחבילות תוכנה מסוימות.

סיפור אמיתי על בגידת סוס טרויאני

בשנת 1996-7, מספר אנשים שחיפשו אתרי פורנוגרפיה מקוונת "חינם" למדו שזה הכל פרט לחינם. אתרי אינטרנט שהציעו תמונות פורנוגרפיות באופן מפורש ב"חינם" פורסמו בחופשיות בקבוצות חדשות של Usenet ודואר אלקטרוני שהופץ ללא הגבלה (Spamming). אלפי משתמשי אינטרנט נלהבים גלשו לאתר "חינם" האמור לעיל, והורידו את "תוכנת החינם" המיוחדת שנדרשה לצפייה בתמונות.

מספר שבועות לאחר הורדת תוכנות החינם שלהם, רבים הזדעזעו לגלות חיובים של מאות דולרים עבור שיחות חוץ לרפובליקה המזרח אירופאית של מולדובה, ליד רומניה.

כפי שהתברר, לתוכנה המיוחדת שנדרשה כדי לעיין בתמונות היו מספר תחבולות באמתחתה. לאחר שהותקנה והופעלה, רכיב סוס טרויאני כיבה את הרמקול שבמודם של המשתמשים, וחייג שיחת חוץ בסתר, שנותבה למולדובה. שיחת הטלפון חויבה לפי $3 לדקה.

גרוע מכך, חלק מהמשתמשים המשיכו לשלם את הסכומים המופקעים לאחר שעזבו את אתר הפורנו וגלשו לדפים אחרים. הנוכלים - שלושה אנשים שהריצו שתי "חברות" בסביבת ניו-יורק - קיבלו כמחצית מרווחי השיחות. ובסופו של דבר הם רימו משתמשי אינטרנט בסך של כרבע מיליון דולר.

ועידת הסחר הפדרלית סגרה את העסק בפברואר 1997, לאחר שקיבלה מידע מ-AT&T, שהבחינה כי מספר גדול במיוחד ממנוייה צברו חשבונות טלפון גדולים בשיחות שהופנו לאותו טלפון במולדובה. לרוע מזלם של המשתמשים צמאי-הפורנוגרפיה, הם הצטרכו לשלם את חשבונות הטלפון שלהם ל-AT&T אף שהוועדה קבעה שמדובר בתרמית. הם אולי יקבלו בסופו של דבר את כספם או לפחות חלקו חזרה, כיון שהמחלקה המשפטית של ארה"ב הקפיאה את כל נכסי החברה.

הלקחים המתבקשים מסיפור סוס טרויאני זה הם ישירים ועקיפים. תחילה, אל תשתמש בתוכנה אם אינך מבין בדיוק מה היא עושה ומהיכן היא באה. שנית, ואולי חשוב יותר, רוב הדברים המוכרזים כ"חינם" אינם כאלה.

וירוסים הבנויים מתוכנות מאקרו

כידוע, מאקרו הוא סדרת פקודות, בחירות תפריט, ו/או פעולות אחרות שהוקלטו מראש. רוב המאקרוס ייחודיים לתוכנה מסוימת (כמו Word או Excel) ומשמשים לפישוט שגרות של פקודות חוזרות. לדוגמה, ניתן להשתמש במאקרו לבנייה של רשימת דיוור מרשימת שם וכתובת פשוטה בקובץ מעבד תמלילים. בעזרת המאקרו, במקום לסמן, להעתיק ולהדביק כל שם וכתובת בנפרד, ניתן לבצע פעולות אלו רק פעם אחת, להקליטם, וכך ליצור מאקרו הניתן להרצה על שמות וכתובות ברשימה. כך תשתמש בהרבה פחות הקשות ותחסוך זמן שיפנה אותך למשימות הבאות.

מאקרוס הם כלי שימושי ביותר, וניתן למצוא רבים מהם להורדה באינטרנט. כמובן מכאן נובע שווירוסים מוחבאים במאקרוס של הרבה תוכנות נפוצות. מאקרו שהוא וירוס עשוי לבצע פעולה שימושית כלשהי, אך בו בזמן הוא גונב או מזיק למידע. כמה וירוסי מאקרו ידועים ביותר שימשו לפלישה ל-Word ול-Excel באלפי מחשבים בסוף שנות ה- 90׳.

המאקרוס עלולים להתקבל דרך דואר אלקטרוני, או שהם יתווספו לתוכנת היעד באמצעות תוכנת סוס טרויאני. בכל מקרה, הם גורמים לכאב ראש רציני בכל מחלקות המחשב.

הפרעה רצה

חלק מהווירוסים מעולם לא מצליחים לעשות את מה שתוכננו לעשות. במקום זאת, הם מפריעים לפעולת המחשב, גורמים לו לצפצף או להודיע הודעות, או מזיזים חלונות על המסך. אולם, יש מספר וירוסים שעושים זאת בכוונה.

גם וירוס ״לא מזיק״ יחסית - שאינו הורס נתונים - הוא גורם הפרעה. תאר לעצמך היתקלות בהערה משפילה או פוליטית בכל פעם שתדליק את המחשב. גרוע מכך,

דמיין שהודעה כזו מופיעה בקביעות אחרי מספר הקשות קבוע בעת שימוש במעבד התמלילים. או דמיין מצב בו המערכת שלך מפסיקה כל כמה דקות ודורשת שתנחש מספר מ- 1 עד 10 לפני שהיא תאפשר לך להמשיך ולעבוד?

וירוסי יישומונים (Applets)

יישומונים הן תוכנות הנשלחות למערכת שלך באמצעות דפי אינטרנט ורצות על הדפדפן. הן כתובות בשפת תסריט מיוחדת הנקראת Java, JavaScript, ו-ActiveX (שים לב שישומוני ActiveX נקראים באופן רשמי **בקרים** [**Controls**]). היישומונים משמשים לכל דבר החל מלחולל טפסים ועד לאספקת חלון תצוגה קטן למידע מיוחד. ניתן להשתמש בהם גם לאנימציה ולניווט באתר האינטרנט.

התפוצה ההולכת וגדלה של יישומוני Java, JavaScript, ובקרי ActiveX יצרה מספר בעיות אבטחה. אולי המקרה המפורסם ביותר ארע בתחילת 1997, כאשר האקרים גרמניים הכריזו על אמצעי לניצול נקודת תורפה ב-ActiveX של מיקרוסופט המאפשר להם פריצה להעברות כספים מסוימות. פירצת אבטחה זו נסגרה בינתיים, אך יש ויהיו אחרות.

אפילו תכונת האבטחה האחת האמיתית של ActiveX חסרת ערך, כיון שרוב גולשי Microsoft Internet Explorer (MSIE) לא יודעים כיצד להשתמש בה. תכונת האבטחה משתמשת בחתימות דיגיטליות (זיהוי באמצעות קוד המסופק באתר האינטרנט, נידון בפירוט בפרק 7) לוודא שהאדם שיצר script נתון או Active X הוא אותו אדם ששולח אותו אליך. אף אם חתימות אלו מיושמות, האקר מנוסה ימצא דרך לעקוף אותן.

בנוסף, חתימות דיגיטליות אינן מונעות ממישהו ליצור בקר ActiveX הרסני העלול למחוק או להרוס קבצים חשובים. גם ל-Java יש פוטנציאל הרסני דומה, אף שהוא כולל גישה חזקה יותר לאבטחה.

כל זה מצביע על כך שפירצות אבטחה אינן פוטנציאל הסכנה היחיד ב-ActiveX וב-Java. גם ActiveX וגם Java יכולים להעביר תוכנות למערכת שלך, ומה שהן יעשו שם פרוץ לחלוטין, כלומר הן יכולות לעשות שם הכל. כך נוצרת יכולת מובנית לאירוח וירוסים. Symantec וחברות אחרות מפתחות או הכריזו לאחרונה על סורקי וירוסים המספקים איתור והגנה בזמן אמת לווירוסים מסוג זה.

שימוש בהגדרות ותוכנות להגנה בפני יישומונים מזיקים

עקב הסכנות הפוטנציאליות שסקרנו, יש לגשת בזהירות לאתרי אינטרנט המאפשרים הורדת יישומוני ActiveX, Java, או JavaScript לדפדפן שלך. כך צריך לנהוג בכלל, לגבי כל תחום יישומי באינטרנט. אם יש לך חשש כלשהו לגבי אתר או היישומון שלו - אל תשתמש באתר.

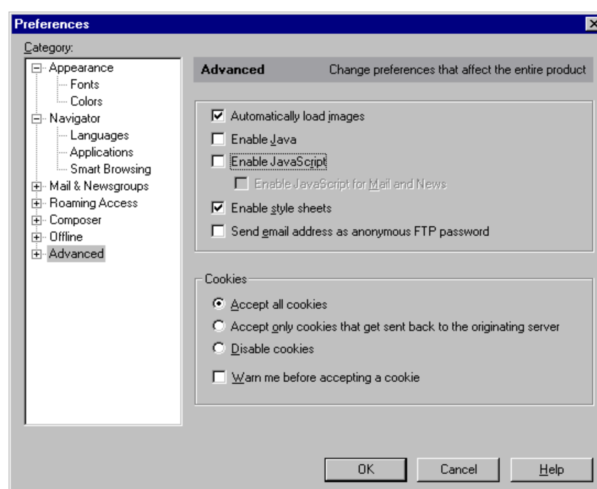
עדיף אף לגלוש באתר כאשר Java, JavaScript, או ActiveX מכובים, כמתואר בסעיף הבא.



כמה אתרי אינטרנט דורשים ששפת Java או שפת תסריט (Script) אחרת תהיה מאופשרת. אם אתה גולש באינטרנט כאשר ActiveX, Java, או JavaScript מכובים, ואתה מגיע לדף שלהפעלתו נדרשים כלים אלה, הפעל את שפת התסריט הרצויה; וחזור וטען את הדף. כך יתאפשרו כל התכונות שהאתר מציע.

ביטול Java, JavaScript או ActiveX עם Netscape

לביטול Java, ו-JavaScript עם Netscape, בתפריט **עריכה** בחר **העדפות (Edit, ו-Preferences)**. תופיע תיבת דו-שיח **Preferences** כמתואר בתרשים 8.1.



תרשים 8.1 ביטול Java ו-JavaScript עם Netscape.

לחץ על **Advanced** והסר סימון מתיבות סימון אפשור Java ו-JavaScript.

המירב שתוכל לעשות לביטול ActiveX ב-Netscape, הוא לבחור ב-**Stop Animations** בתפריט **תצוגה (View)**.

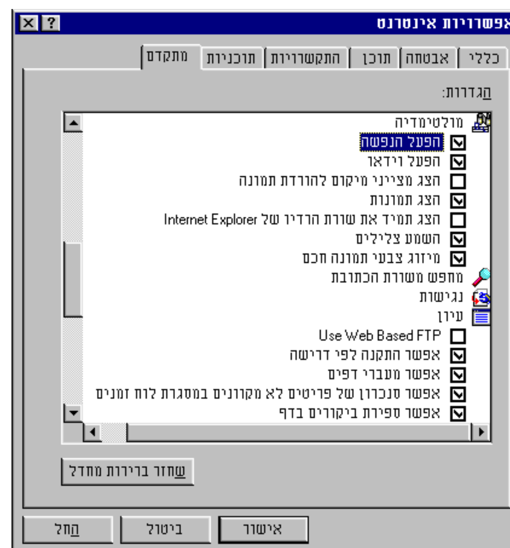
ביטול Java, JavaScript או ActiveX עם Internet Explorer

בגירסה 5 של Microsoft Explorer, פתח את תפריט **כלים**, ולחץ על **אפשרויות אינטרנט**. לחץ על כרטיסיית **אבטחה** בחלון **אפשרויות אינטרנט**, ולחץ על לחצן **רמה מותאמת אישית** בתחתית תיבת הדו-שיח **אפשרויות אינטרנט**. עבור גירסה 4, פתח את תפריט **עריכה**, ולחץ על **אפשרויות אינטרנט**. לחץ על לחצן **אבטחה**; עתה לחץ על לחצן אפשרויות **רמה מותאמת אישית** ולחץ על **הגדרות**. עלעל מטה ל-Java ופתח אותו; סמן את תיבת הסימון **בטל Java**. תיבת הדו-שיח של האבטחה תוצג, כמתואר בתרשים 8.2. כאן, לחץ על לחצן אפשרויות **בטל** המתאים לכל אפשרויות Java.

לביטול ActiveX, פתח את תפריט **כלים** ובחר **אפשרויות אינטרנט**, לחץ על **מתקדם** ובחר ב**מולטימדיה** והסר סימון מתיבה בשם **הפעל הנפשה**, כמתואר בתרשים 8.3.

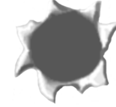


תרשים 8.2 שימוש באבטחת Explorer לביטול Java

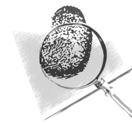


תרשים 8.3 ביטול אנימציית (הנפשה) ActiveX הוא רעיון טוב

תוכל גם להגדיר אפשרויות אלו באמצעות **התחל**, בחירה ב**הגדרות**, לחיצה על **לוח בקרה**, ובחירה ב**אפשרויות אינטרנט** (שים לב שתיבת הדו-שיח שתופיע תיקרא **מאפייני אינטרנט** ולא **אפשרויות אינטרנט**).



שים לב שמיקרוסופט בחרה שלא להכיר ב-Javascript באופן רשמי - אף שפקודות JavaScript עובדות עם דפדפן Explorer. לכן, לרוע המזל, אין כל אפשרות לבטל את ביצוע פקודות JavaScript ב-Explorer.



תוכנות Java "מזיקות" רבות הן תוצאה של תכנות לא מיומן ו/או אי בדיקת יישומון Java ביותר מסביבה אחת. הרצון שיהיו כל מיגוון התנועות, הצבעים והפעולה על דפי האינטרנט גורם שמתכנתים חסרי כישורים יתרכזו יותר באיך הדף ייראה על מסך המחשב שלהם מאשר על אופן כתיבת הקוד. התוצאה היא שהדפדפן או אף מערכת ההפעלה יינעלו או יקרסו עקב מספר הפריטים שיש לטעון כדי להציג את הדפים. כיון שאין אף אחד שמאשר או בודק בדרך אחרת את איכות אתרי האינטרנט, זו סיבה נוספת לגלוש כאשר java אינה פעילה (אין כל ארגון מרכזי הבוחן או משגיח על איכות או תוכן אתרי אינטרנט. שירותי ההערכה הקיימים מסתמכים בעיקר על שיפוט אישי).

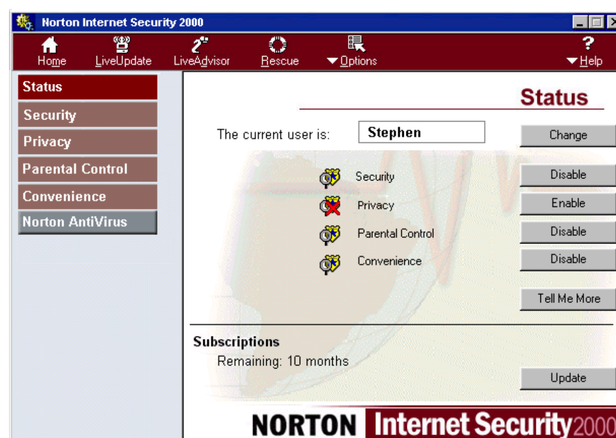
McAfee Guard Dog

אם אינך רוצה לטרוח ולשנות את הגדרות הדפדפן, כדאי לשקול את תוכנת McAfee Guard Dog. התוכנה נועדה להגן על המערכת מווירוסים וסוסים טרויאניים העלולים להגיע דרך יישומוני Java ובקרי ActiveX.

Guard Dog גם סורקת ומסירה וירוסים מתוכנות שהורדו וצירופי דואר אלקטרוני. בנוסף, היא יכולה לחסום Cookies, לנקות עקבות שהשארת במחשב בעת גלישה באינטרנט, ולהגן על מידע רגיש. המוצר מתעדכן במלואו באתר המוציא לאור: http://www.McAfee.com.

Norton Internet Security 2000

Norton Internet Security 2000 תוכננה לעצור וירוסים והתקפות אחרות דרך יישומוני java, בקרי ActiveX, ואפילו צ'טים של IRC. כפי שמתואר בתפריט הראשי בתרשים 8.4, Norton Internet Security 2000 מאפשרת אמצעי בקרה להורים להגבלת גישה של ילדיהם לאתרי אינטרנט מסוימים.



תרשים 8.4 התפריט הראשי של Norton Internet Security 2000

תכונות נוספות של Norton Internet Security 2000 כוללות הגנת דואר אלקטרוני, נתוני כרטיס אשראי, ומידע פרטי נוסף. תוכל גם להגדיר פרופילים רבים למשתמשים ולחסום פרסום. בנוסף, Norton Internet Security 2000 כוללת את Norton AntiVirus 2000.

למידע נוסף ראה אתר: http://www.symantec.com/sabu/nis/index.html

כיצד וירוס חודר למערכת שלי?

לרוב, וירוס חודר למערכת תחת מסווה של תוכנה או מאקרו. לדוגמה, נניח שהורדת קובץ המתיימר להיות משחק בשם FUNGAME.EXE. בעודך מריץ אותו ומנסה להבין כיצד לשחק את המשחק, התוכנה עלולה לעבוד ברקע ולמחוק את כל הקבצים בתיקיה הנוכחית - או כל התיקיות - או להצמיד וירוס לקבצי האתחול (כפי שצוין קודם, סוס טרויאני הוא שם מתאים ביותר לווירוס מסוג זה).

רוב הווירוסים ותוכנות הסוס הטרויאני מוסוות כתוכנות ציבוריות או שיתופיות כדי לעודד הפצתם. כפי שצוין קודם, חלקן מוסוות או משובצות בהעתקים חוקיים ולא חוקיים של תוכנות מסחריות. בנוסף, חלק מתוכנות הווירוס תוכננו לנצל את החמדנות האנושית, ומסוות עצמן כתוכנות המסייעות לחדור לאתרי אינטרנט לקבלת זמן גלישה חינם או שירות מקוון, או מציעות הטבה בלתי סבירה אחרת.

הורדות מקוונות (Download)

עבור רוב הווירוסים, הורדת חומר מקוון היא דרך החדירה העיקרית למחשב, גם כיון שכל כך הרבה קבצי מחשב מגיעים היום באמצעות טעינה מקוונת. אולם, הסיבה העיקרית היא שקובץ נגוע בווירוס מדביק ומתרבה מהר יותר בצורה מקוונת מאשר בכל דרך או מדיה אחרת. כיון שאלה היוצרים וירוסי מחשבים רוצים בחשיפה מירבית, רובם רואים בעולם המקוון אמצעי הפצה עבור יצירותיהם.

לווירוסים המתפשטים בצורה מקוונת יש את הסיכוי הטוב ביותר לחיים ארוכים. לוקח זמן רב מרגע הגילוי הראשון של וירוס מקוון ועד להשמדת אחרון הווירוסים. רבים אינם מודעים למקורות מידע מקוונים המדווחים על וירוסים, וחלקם טוענים את הווירוס במקום אחר, שמים אותו בשירותים מקוונים או אתרי אינטרנט, ושם קורבנות תמימים אחרים טוענים אותו. כל טעינה חדשה מכפילה את מספר המחשבים הפוטנציאליים החשופים לווירוס. קורה אפילו שאנשים שולחים אותם בדואר אלקטרוני לחבריהם.

קבצים מצורפים (Attachments)

וירוסים יכולים להגיע עם קבצי תוכנה המצורפים להודעות דואר אלקטרוני. קריאה רגילה של הודעה לא תפעיל את הווירוס; אולם, פתיחת הקובץ הנגוע המצורף ו/או הרצת התוכנה או המאקרו המצורפים כן יגרמו להדבקה.

התברר שתדירות צירוף תוכנות להודעות דואר אלקטרוני גדלה משמעותית בתקופות של חגים. אף שקבצים מצורפים אלה עשויים להיראות תמימים, מומלץ פשוט למחוק אותם. גם אם אתה יודע מי שלח את הקובץ אליך, צא מתוך הנחה שהם כנראה שולחים הלאה משהו שהגיע אליהם באותה צורה ואולי לא בדקו אם הקובץ נגוע בווירוס.

קבצים משותפים ברשת

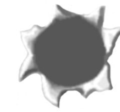
קבצים משותפים ברשת מפיצים וירוסים מהר מאוד. למד את מדיניות מנהל המערכת לגבי קבצים משותפים, איומי וירוסים, ונושאים קרובים. הימנע מהרצת קבצים שהגיעו עם דואר אלקטרוני, והודע למנהל המערכת מייד אם אתה מוצא קובץ חשוד.

דיסקטים משותפים

וירוסים המופצים על דיסקטים מתרבים די לאט. בעלי מחשבים לא משתפים תוכנות על דיסקט כמו פעם כיון שעכשיו הכל מקוון ונגיש. אך הפצת וירוסים באמצעות דיסקטים טרם הוכחדה לחלוטין.

חבר לעבודה עלולים להעביר לך תוכנה נגועה בווירוס לפני שתזהה אותו, או מישהו עלול להפיץ העתקי תוכנה שיתופית נגועה.

במקרים הנדירים שווירוס מתגנב לדיסקט או תקליטור מסחריים, ניתן להשמיד כמעט כל עותק שלו (הדבר אכן קורה. יותר מפעם אחת עובד לא מרוצה או סתם ליצן שינה מוצר תוכנה מסחרי לפני שכפולו).

	עתה, כאשר צורבים של תקליטורים זמינים, עליך להיזהר בהרצת תוכנות שנצרבו על תקליטור בצורב ביתי.

הגנה בפני וירוסים

מניעה היא תמיד התרופה הטובה ביותר. תוכל לעשות רבות למנוע חדירת וירוסים למידע או למערכת.

לפני שנמשיך, יש לציין שהמחשב לא יכול להידבק מווירוס מעצם פעולת ההתחברות לספק שירותים מקוונים או אינטרנט. וירוסים ותוכנות סוס טרויאני אינם מסוכנים אלא אם הם **הורצו**.

עם זאת, להלן כמה טיפים למניעת וירוסים:

- אם תוכנת הגנה נגד וירוסים (אנטי-וירוס) אינה מותקנת על המערכת שלך, התקן תוכנה כזו ועדכן אותה תכופות.
- אם תוכנת האנטי-וירוס שלך מאפשרת הגנה אוטומטית רציפה כל הזמן, שקול להפעיל תכונה זו. כך ייסרקו כל ההורדות, הקבצים והתוכנות במערכת.
- היזהר לגבי מה שאתה מוריד. אם יש לך שאלה לגבי תוכנה ממקור להורדת תוכנות, שאל את מנהל האתר (Sysop) (האדם שמנהל את אתר האינטרנט או השירות המקוון), אם הוא ניסה את התוכנה ומצא שהיא בטוחה. שאל משתמשים אחרים על התוכנה (ככלל, אם תוכנה הורדה פעמים רבות - מוני הורדות ניתנים לצפייה בכמה מערכות - ולא ראית תלונות עליה בפורומים, יש להניח שבטוח להוריד את התוכנה).

- אם אתה מקבל דואר אלקטרוני עם קובץ מצורף ממישהו שאינך מכיר, מחק את הקובץ מייד. אם הקובץ הגיע ממישהו מוכר, שאל אותו היכן השיג את הקובץ והאם סרק אותו בתוכנת אנטי-וירוס (רצוי שתסרוק אותו גם אתה).
- אם חבר לעבודה נותן לך דיסקט עם תוכנה עליו, שאל אותו האם הוא יודע שהתוכנה בטוחה? האם הריץ את התוכנה? האם סרק אותה בתוכנת אנטי-וירוס? האם ידוע לו מה מקור התוכנה?
- לפני הרצת התוכנה, בחן את קבצי הארכיב שלה בקפידה וקרא את קובץ READ.ME או קבצי טקסט דומים - יוצרי תוכנות ציבוריות או שיתופיות לעיתים קרובות כוללים תיאור, עם גדלי קבצים, של הקבצים בארכיב תוכנה. אם אתה רואה קבצים שאינם כלולים בתיאור, אל תפעיל את התוכנה.
- אף אם אין חשד מיידי לגבי תוכנה, סרוק אותה באמצעות אחת מתוכנות האנטי-וירוס (ניתן להגדיר כמה תוכנות כאלו לסריקה אוטומטית של ארכיבים ותוכנות בעת הורדתם).
- אם יש לך חשד שיש וירוס בתוכנה, **אל תשתמש בה**. סרוק אותה עם אחד או יותר מתוכנות האנטי-וירוס.
- כאשר אתה קונה תוכנה מסחרית, ודא שחותמת המפעל לא נפרצה - ושהאריזות הפנימיות והחיצוניות של התקליטור שלמות.

הקפד להתעדכן

כבכל איום, התעדכנות קבועה בנושא וירוסים היא הגנה חשובה. מקור המידע הטוב ביותר בקשר לווירוסים הוא האינטרנט.

"אתרעות וירוסים" מופצות תכופות באמצעות דואר אלקטרוני, אך רבות מהן הן תרמיות (ראה בהמשך "אל תיבהל: תרמיות וירוס", בסוף פרק זה). כדי להתעדכן בבעיות וירוס אמיתיות, ניתן לגשת לאתר של McAfee (http://www.McAfee.com) ושל Symantec (http://www.symantec.com) לעיתים תכופות. כל אחד מהם מספק ארכיבי מידע על וירוסים של מחשבים, בנוסף לעדכונים על איום הווירוס האחרון המאיים על משתמשי מחשבים. שניהם גם מספקים מידע על תרמיות הווירוס האחרונות.

משאבים מקוונים נוספים על וירוסים ואנטי-וירוסים ניתן למצוא בפורומים שונים באתר: www.iol.co.il למשל.

תוכנות אנטי-וירוס

לפני שנפרט תוכנות אנטי-וירוס, להלן פירוט היכולות העשויות להיות קיימות בתוכנות אלו:

- חיפוש בתוכנות החשודות בווירוס, אחר הודעות חשודות מן הסוג המוצג על ידיהן לעיתים תכופות.
- בחינת קבצי מערכת הפעלה לאיתור שינויים.
- חסימת תוכנה החשודה בווירוס, ממתן פקודה העלולה להיות מסוכנת.
- הכנסת תוכנות וירוס ל"בידוד" כך שלא ניתן יהיה להפעילן.
- הסרת וירוסים מהמערכת.
- תיקון קבצים שניזוקו מווירוס (אלה כוללים תוכנות חוקיות, שלעיתים נוהגות כ"מארחות" לווירוסים, בנוסף לקבצי נתונים).
- סריקת קבצים מורדים וקבצים שהגיעו עם דואר אלקטרוני לאיתור וירוסים.
- סריקת כוננים, תיקיות ו/או קבצים לפי דרישה, או בתזמון קבוע.
- עדכון עצמי בתזמון קבוע, או לפי דרישה.
- הגנה אוטומטית על המערכת תוך כדי השימוש בה, מעקב אחר תוכנות, קבצים ומשאבי מערכת.

כבר הזכרתי שתי תוכנות אנטי-וירוס המתמקדות בהגנת המערכת מאיומי אינטרנט. עתה נבחן את תוכנות האנטי-וירוס הכלליות הטובות יותר.

אנטי-וירוס Dr Solomon

תוכננה זו תוכננה במיוחד עבור Windows 95, וקיימת גם גירסה עבור Windows 95/98 ו-Windows NT. התוכנה מתמחה בבדיקת ארכיבים לגילוי וירוסים. סוגי הארכיבים כוללים ARC., ARJ., Cryptcom, Diet, Ice, LZH, MS Compress, Pklite, ZIP., וארכיבים לפרישה-עצמית שנעשו באמצעות LZExe ו-ZIP2EXE. היא גם מגלה וירוסים במאקרוס.

התוכנה כוללת עדכונים חינם לעד. למידע נוסף, ראה http://www.McAfee.com

McAfee VirusScan Online

McAfee מפעילה שירות מנויים מקוון לסריקת וירוסים, בנוסף לניתוח ביצועי מחשב, ומקור עצות ומידע על Windows. הדף הראשי של השירות באינטרנט, כמתואר בתרשים 8.5, ייתן לך מושג על ההיצע.

שירותים אלה זמינים באמצעות מנוי באתר :

.http://www.McAfee.com/centers/anti-virus/virus_help_me.asp



תרשים 8.5 שירות מקוון לסריקת וירוסים של McAfee.com

McAfee Virus Scan Deluxe ל-Windows 95/98

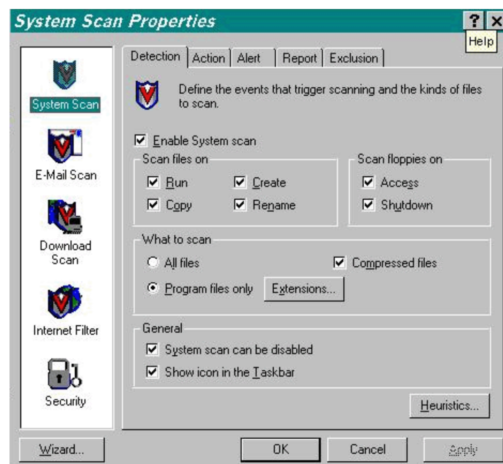
Virus Scan Deluxe של McAfee.com, נועדה לגלות וירוסים באינטרנט, ברשתות, ובתוכנות. כמו כן יש לה יכולת לסרוק קבצים מצורפים עם דואר אלקטרוני לפני פתיחתם. היא יכולה גם לסרוק הורדות, כולל קבצי ZIP., ARC. ו-ARJ, בנוסף לארכיבים לפרישה-עצמית. Virus Scan Deluxe גם מאתרת את כל סוגי הווירוס, כולל אלה שבספקטור האתחול, קבצים פולימורפיים, חמקניים, מוצפנים, ומאקרו. כבונוס נוסף, היא גם מגלה וירוסים של MS Office 97/2000. החבילה כוללת עדכוני חינם לעד דרך אתר McAfee.

תוכנה זו מכילה גם שתי תוכנות שירות : First Aid (עזרה ראשונה) ו-Oil Change (החלפת שמן). לא כדאי להתעסק עם אלו בהתחלה. First Aid משנה את הדפדפן והגדרות שמתייחסות אליו במחשב. Oil Change מוצאת עדכונים של תוספי תוכנה (Plug-ins) מקוונים אוטומטית ומתקינה אותם.

ממשק המשתמש, כמתואר בתרשים 8.6, קל לשימוש.

בנוסף לאמור לעיל, Virus Scan Deluxe כוללת עדכון חינם לעד. התוכנה קיימת כגירסה עצמאית, וגם כחלק מחבילת McAfee Utilities Deluxe ו-McAfee Office 2000.

למידע נוסף, ראה http://www.McAfee.com.



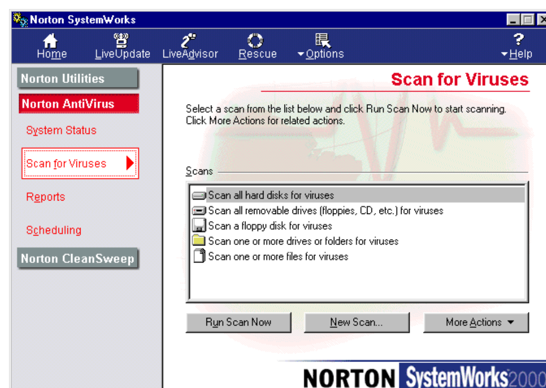
תרשים 8.6 ממשק משתמש של Virus Scan Deluxe

Norton AntiVirus 2000

Norton AntiVirus 2000 (NAV 2000) היא אולי תוכנת האנטי-וירוס הידועה ביותר הקיימת כיום. היא זמינה לבד או כחלק מחבילת Norton SystemWorks 2000. Norton AntiVirus 2000 מציעה מספר רמות הגנה ומיגוון אפשרויות הפעלה הכוללים:

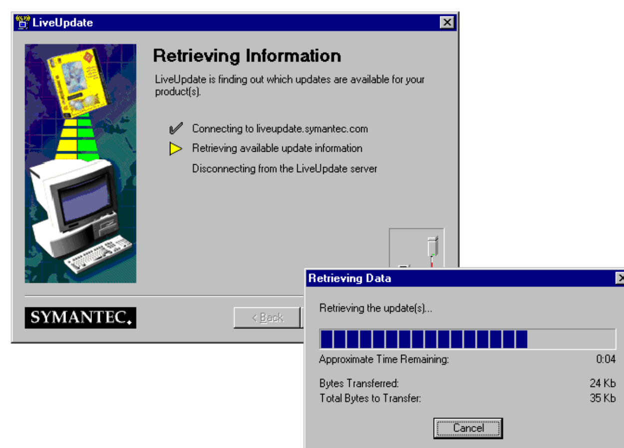
- סריקת וירוסים ידנית בקבצים ייעודיים, תיקיות, וכוננים (כולל דיסקטים ותקליטורים).
- סריקה ידנית של כל מערכת ההפעלה.
- דוחות מלאים.
- הגנה אוטומטית בעת שימוש במחשב.
- סריקה אוטומטית של דואר אלקטרוני ותוספות המצטרפות אליו.
- סריקה של הורדות לגילוי וירוסים (ארכיבים ותוכנות עצמאיות).
- הגדרות וירוס ניתנות לעדכון.

כמתואר בתרשים 8.7, NAV 2000 מציעה מיגוון הגדרות רחב בכל אפשרויות ההגנה.



תרשים 8.7 Norton AntiVirus 2000 בעלת גמישות הפעלה רבה

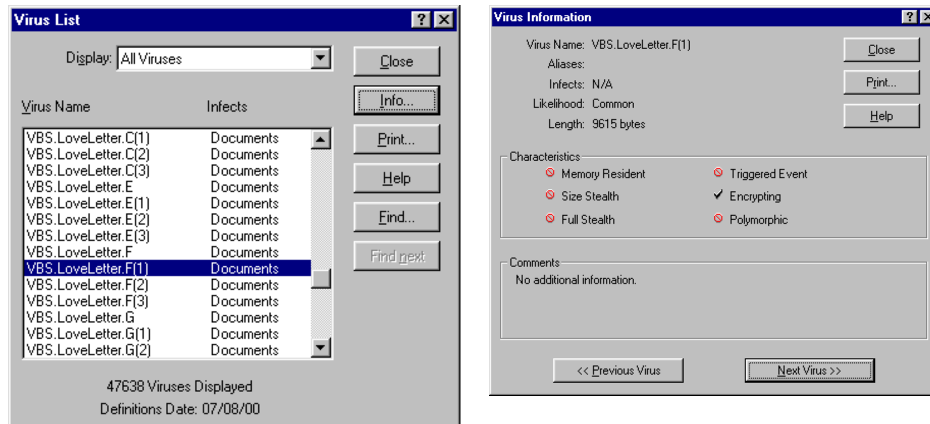
תוכל לתזמן סריקה כל מערכת ההפעלה או סריקה חלקית בימים/שעות ספציפיים או לגרום לתוכנה להזכיר לך לבצע את הסריקה. כמו כן היא תזכיר לך לעדכן את הגדרות הווירוס שלך, אם תרצה. העדכונים נעשים בצורה מקוונת (תרשים 8.8) באתר Symantec, ו-Norton AntiVirus 2000 משווקת עם שירות מנוי חינם לעדכונים של שישה חודשים (דמי המנוי לאחר מכן מזעריים).



תרשים 8.8 עדכון מקוון של Norton AntiVirus 2000

בנוסף, תוכל להתאים באופן אישי דוחות ואתרעות, סריקה אוטומטית באתחול, סריקת קבצים שהגיעו יחד עם דואר אלקטרוני, ועוד. תוכל גם לקבוע אם התוכנה תופעל אוטומטית בעת השימוש במחשב. אם היא תוגדר לפעולה אוטומטית, Norton AntiVirus 2000 תנטר וירוסים בעודך עובד - אפילו תבדוק קבצי Zip תוך כדי פתיחתם. התוכנה גם מוסיפה אפשרויות סריקת וירוסים לתפריט הלחיצה-ימנית על העכבר (כאשר אתה רוצה לבדוק מאפייני קובץ או תיקיה).

Norton AntiVirus 2000 מספקת גם רשימה מקיפה של יותר מ- 50,000 וירוסים, עם פרטים על כל אחד מהם. כמתואר בתרשים 8.9, זה הוא כלי יעיל העוזר בהבנת וירוסים, או פשוט כדי לספק את סקרנותך.



תרשים 8.9 מסד נתוני הווירוסים המובנה בתוך Norton AntiVirus 2000.

אם היא מזהה וירוס, Norton AntiVirus 2000 מתריעה ומאפשרת לך להחליט אם למחוק, לתקן, להכניס להסגר, או להתעלם מהקובץ עם הווירוס. אם תאפשר לתוכנה לתקן את הקובץ האמור (האפשרות המומלצת), היא מוחקת את הווירוס.

מידע מפורט יותר אודות Norton AntiVirus 2000, ראה באתר:

http://www.symantec.com/nav/index.html

אל תיבהל: תרמיות וירוס

נראה שבכל שנה יש לפחות תרמית וירוס אחת. דוגמאות שאירעו לאחרונה כוללות את וירוס Good Time (מקורו בסוף 1994); מדובר במספר וירוסים שהיו אמורים להיכנס לפעולה בחגים מסוימים ולהרוס את כל קבצי הנתונים במחשב; היו כאלה שהיו אמורים להיות מופצים באמצעות הצמדות לדואר אלקטרוני ולהרוס קבצים בעת קריאת ההודעות שהתקבלו; ב- 1996 וב- 1997, הופיעו וירוסים שאמורים היו להיות "מוחבאים" במאקרוס של מעבדי התמלילים.

בעוד שכל הווירוסים הללו התגלו כתרמיות, הם גרמו לבזבוז זמן רב ורוחב פס באינטרנט. הם גרמו לאנשים לכלות את זמנם בחיפוש אחר הגנות או תרופות לבעיות שלא היו קיימות. בסופו של דבר, השמועות והתרמיות של הווירוסים היו יעילות כמו הווירוסים האמיתיים בכך שהן גרמו לבזבוז זמן ותפיסת משאבים באופן דומה.

אין לדעת אם כל אחד מווירוסים אלה היה תרמית מכוונת או סתם מיתוס. בהחלט, אנשים ממציאים תרמיות וירוס מסיבות שונות, ואנשים חסרי ידע מפיצים שמועות לפעמים בלא כל כוונה.

בעוד שאיני ממליץ על התייחסות לא רצינית לנושא הווירוסים, כדאי לבדוק קצת באשר לאמינות איום וירוס לפני נקיטת פעולה כלשהי או בזבוז זמן רב בחיפוש אחר הפעולה הנדרשת. במקורות שצוינו קודם - McAfee, Symantec, ופורומים הנוגעים לווירוסים - יש את המידע העדכני ביותר לגבי וירוסים או תרמיות וירוסים.

אתרים חשובים במיוחד לתחום זה הם:

- אתר הבית של Computer Virus Myth Home Page: http://kumite.com/myths/
- ספריית המידע של McAfee על וירוסים/תרמיות:

http://vil.McAfee.com/hoax.asp

- מרכז מחקר אנטי-וירוס של Symnantec: http://www.symantec.com/avcenter/

עכשיו כשאתה מכיר יותר את הווירוסים בהם אתה עלול להיתקל ויודע כיצד למנוע אותם, ויודע מה ערך העירנות לסכנות אפשריות, אמיתיות או מדומות, נוכל להתקדם למשהו שאינו תרמית - ביטחון ופרטיות באינטרנט.

פרק 9



ביטחון ופרטיות באינטרנט

מה בפרק:

- סכנות באינטרנט
- איך הגענו לכאן?
- נושאים בסיסיים באבטחה מקוונת
- אבטחת מידע מקוונת
- אבטחת הורדות (Downloading)
- טשטוש עקבות מקוונות

עכשיו הגיע הזמן לטפל באיום הגדול - האינטרנט!

עקב הפחדה תקשורתית, יותר אנשים פוחדים מהאינטרנט מאשר הם פוחדים מסופות, רעידות אדמה, וחמסינים גם יחד. אך נראה שזהירות אינה מתלווה תמיד לפחד, כיון שיותר אנשים מאי פעם בעבר הם קורבנות להטרדות, רמאויות, ושרלטנים בכלל, והאינטרנט היא רק סביבת פעולה נוספת.

הסיבה שאנשים כה רבים הם קורבנות מקוונים היא בדרך זו או אחרת, פשוטה מאוד: הם חסרי ידע כיצד להגן על עצמם בעולם המקוון. פרק זה דן בכך.

אולם, תחילה נסקור כמה מהסכנות המקוונות, ונקבל מעט רקע על האינטרנט והאנשים המשתמשים בו. לא דברים טכניים - רק מספיק מידע כדי לדעת מה נמצא שם, ומעט היסטוריה על איך הוא התפתח.

לאחר מכן נתבונן בנושאי אבטחה מקוונת בסיסיים ואיך לשמור על פרופיל נמוך ובכל זאת ליהנות מהאינטרנט. לבסוף, אסביר כיצד למנוע השארת את עקבות נוכחותך המקוונת, כך שאיש לא יוכל לדעת היכן היית גם לאחר שהמחשב אינו מקוון.

שישים שניות על הסכנות באינטרנט

ראית את זה בחדשות שוב ושוב: מישהו נופל קורבן לתרמית של נוכל אינטרנט; מישהו אחר מנוצל באמצעות רומן מקוון; השכן הסתבך בחובות כספיים לאחר שנרשם לאתרי פורנוגרפיה מקוונים - או האם זה היה הבן של השכן שגנב את מספר כרטיס האשראי והשתמש בו להיכנס לכל אתרי האינטרנט המפוקפקים? אלה סיפורים ידועים, אך לרוע המזל הם נשנים וחוזרים.

יש גם סיפור על בחור שהיה שקוע עד צוואר ברומן מקוון עם אישה שמעולם לא פגש. יום אחד אשתו הסתכלה במקרה בתיבת הדואר האלקטרוני שלו. שוב, הסיפור חוזר על עצמו, אך הקשיים התעוררו בעולם הרגיל ולא בעולם המקוון.

כמובן שאפשר להסתבך בעולם המקוון כשאתה מקוון ובלתי מקוון. הסכנה קיימת, בין אם דרכיך מצטלבות עם האנשים הלא נכונים בעולם המקוון, או שאינך מרגיש בנוח כאשר עקבותיך המעידים היכן גלשת ומה עשית, מוחבאים אי שם במחשב שלך וזמינים לכל אדם. למזלך, ניתן למזער סיכונים אלה. להבנה טובה יותר בפני מה אתה עומד, אנו נתבונן היכן אנו נמצאים ואיך הגענו לכאן.

שורש הבעיה

אנשים מתייחסים לעולם המקוון כמשהו שונה לחלוטין ומנותק מהעולם האמיתי - וזה מה שגורם בעיות. אנשים שלא היו חולמים לתת את כתובתם לזר, או להתחיל ויכוח עם זרים בקניון, עושים זאת בעולם המקוון. הם מקלים על אחרים למצוא אותם ולהציק להם ומעוררים כעס בהערות שלא לעניין. רבים יוצרים הידברות עם אנשים שהיו נמנעים מהם כמו ממגפה בעולם האמיתי. מדוע? אולי משום שהכל נראה כה לא אמיתי ותחת שליטה - אבל האם זה באמת כך?

ישנם שני היבטים בעולם המקוון התורמים את חלקם לרוב הבעיות המקוונות. הראשון הוא הרגשת האלמוניות. אנשים לא יודעים מי אתה ולא רואים אותך, אז אתה יכול לעשות או לומר ככל העולה על רוחך, נכון?

ההיבט השני הוא חוסר המציאות או הסוריאליזם של יישות האינטרנט. עבור רבים, אנשים שהם פוגשים בעולם המקוון הם אמיתיים בערך כמו דמויות במשחק מחשב. מכאן שרוב האנשים מתעלמים מהאפשרות שמישהו שהם פוגשים בעולם המקוון יוכל להזיק להם בדרך כלשהי. זה גם מקל על אנשים להטריד ולגנוב מאנשים מקוונים - בסופו של דבר, הפשעים שלהם אינם אמיתיים עבורם.

אולם, תוכל להימנע מצרות אלו על ידי הקפדה עם מי אתה יוצר קשר ומה אתה עושה בעולם המקוון. ניתן להימנע מאלה שיש להם נטייה להטריד לשם שעשוע או הפקת רווח, שלא לדבר על אלה שיותר ממוקדים במטרותיהם המקוונות הנפשעות: אורבים לטרף, אומני הונאה, ועבריינים אחרים.

נושאי אבטחה מקוונת בסיסיים

נושאי האבטחה המקוונת הבסיסיים ביותר כרוכים בדברים שאתה עושה או משתמש בכל פעם שאתה מקוון. שער הכניסה לאמצעים אלה היא הסיסמה שלך בשילוב עם קוד המשתמש. בנוסף, עליך להקפיד על אבטחת מספרי כל כרטיסי האשראי שלך.

סיסמאות

סיסמאות הן המפתח לחייך המקוונים. אם למישהו יש את הסיסמה/סיסמאות שלך, הוא יוכל ל**היות** אתה. אם מישהו אחר ישתמש וייגש לחשבון ספק האינטרנט שלך ולאתרים עם הסיסמה שלך, הוא יוכל לבצע את הדברים הבאים:

- לקרוא את הדואר האלקטרוני שלך
- לשלוח דואר אלקטרוני בשמך
- לשים הודעות בפורום בשמך
- לרכוש מוצרים ברשת (אם החיוב מתבצע דרך ה- ISP שלך).

אף שרבים נכשלים בכך, הגנה על סיסמתך קלה יחסית. כל שעליך לעשות הוא לזכור אזהרות אלו, ולנהוג בהתאם:

1. אל תיתן את סיסמתך לאיש בביתך או בעבודתך.
2. **לעולם** אל תיתן את סיסמתך באמצעות דואר אלקטרוני או בצ'ט, לא משנה מה התירוץ הניתן על ידי האדם המבקש אותה (עבריינים רבים מוציאים את הסיסמה מאנשים על ידי כך שהם מציגים את עצמם כעובד של ספק אינטרנט או שירות מקוון אחר).
3. קבע לך סיסמאות ארוכות וייחודיות, לפחות 8 תווים המורכבים מאותיות וספרות. כגון K9R3781. הימנע משימוש בתאריך הלידה של בנך, השם של אשתך, שם הכלב, וכדומה; קל מדי לנחש סיסמאות כאלו.
4. אל תרשום את הסיסמה - **זכור** אותה.
5. הימנע מהורדה והרצת תוכנות המצורפות לדואר אלקטרוני, ותוכנות המוצעות באתרי אינטרנט הנראות יותר מדי טוב מכדי להיות בחינם. יש סיכוי טוב שתוכנות מסוג זה מתוכננות לפרוץ ולגלות את הזיהוי האלקטרוני והסיסמה שלך ולשלוח אותן לגנב מקוון (ראה פרקים 1 ו- 8 למידע נוסף על תוכנות סוס טרויאני ונושאים הקשורים בכך).

האם למישהו יש את סיסמתך?

עד שגנב משנה את סיסמתך או עושה משהו בולט בשירות המקוון, לא תדע אם סיסמתך נפרצה. אם אתה משתמש בשירות מקוון בו ניתן לעשות שינויים לכרטיס שלך, לא תדע שיש לך בעיה עד שמגיע החשבון. כך תוכל לבדוק אם סיסמתך נגנבה:

- ❖ אם ספק האינטרנט שלך או השירות המקוון מספק אמצעי לבדיקת זמן התקשורת שלך, השתמש בכך לעיתים. אולי תגלה ש"אתה" היית מקוון בזמן שלא היית.
- ❖ דואר אלקטרוני מוזר המתייחס לנושאים שאין לך ידע בהם, במיוחד מאנשים שאינך מכיר, יכול להעיד שמישהו אחר משתמש בחשבון שלך (ואולי אף מקבל ושולח דואר אלקטרוני).
- ❖ ניסיון להתחבר לשירותים מסוימים וקבלת הודעה שאתה כבר מקוון מהווה אות אזהרה (אולם, זה לא תמיד מעיד שמישהו אחר מקוון בשמך. אם אתה מקבל הודעה כזו כאשר אתה מנסה להתחבר שנית לאחר שנותקת מהרשת, לרוב המערכת פשוט עוד לא הטמיעה את העובדה שאתה לא מקוון).
- ❖ אם ספק האינטרנט מודיע לך שאתה מתחבר בו-זמנית מכמה מקומות, זו עדות לבעיה (כמובן, אם אתה באמת עושה זאת, תקבל תלונות; ספקי אינטרנט לא אוהבים שמשתמש אחד צורך יותר משאבים משנדרש).
- ❖ אם אתה מוצא הודעות שלא שלחת בפורום - או תשובות להודעות שלא שלחת - כנראה שמישהו משתמש בסיסמתך.
- ❖ אם אתה מקבל הודעה מספק האינטרנט על כשלים רבים בהתחברות, זו בהחלט יכולה להיות עדות שמישהו מנסה לפרוץ לחשבון שלך על ידי ניחוש סיסמתך.

מה לעשות אם סיסמתך נפרצה

באופן אידיאלי איש מעולם לא ישיג את סיסמתך, כיון שיישמת את העצות שבסעיף הקודם. אולם, אם מסיבה כלשהי מישהו השיג את סיסמתך, פעל כדלקמן:

- ❖ אם ניתן, שנה את סיסמתך מייד. אם אינך יכול להתחבר, התקשר לשירות הלקוחות של ספק האינטרנט או השירות המקוון (היה מוכן לזהות את עצמך, לרוב על ידי פרט אישי כלשהו, שנדרש ממך בעבר כאשר נרשמת לשירות).
- ❖ אם לא ניתן לשנות את סיסמתך, התקשר לשירות הלקוחות של ספק האינטרנט שלך והודע להם מה קרה. אם נוספו חיובים שאינם שלך לחשבון, אולי תוכל לזכות חלק מהם.
- ❖ אם אתה מזדמן לפורומים ומוצא הודעות כביכול שלך, שלח הודעה שסיסמתך נפרצה ושאינך אחראי להודעות שנשלחו מתאריך מסוים ועד היום.
- ❖ שנה את סיסמתך שוב.

כמובן, עשה את מירב המאמצים שאיש לא ישיג את סיסמתך.

הזהות שלך

הרעיון שמישהו שאתה מכיר יכול להוות סכנה עבורך אולי נשמע מגוחך, אבל זו עובדה שעליך לשמור על פרטיותך בקפידה בעולם המקוון. מדוע? כיון שככל שמישהו יידע עליך יותר, כך קל לו יותר לשלוח יד ולגעת בך בעולם האמיתי.

האם מספר הטלפון שלך רשום במדריך הטלפונים? האם שם המשפחה שלך ייחודי? כך או כך, קל יחסית לאתר אותך אם יודעים באיזה עיר אתה גר. כמו כן לא רצוי לתת פרטים על מקום עבודתך.

מדוע כל זה חשוב? שקול את התוצאות של המקרים הבאים:

- אתה עלול לעלוב במישהו בטעות, והוא עלול לחפש "נקמה" על ידי הטרדה (הערות תמימות כביכול יכולות להתפרש בצורה לא נכונה. בנוסף, יש אנשים מקוונים המטרידים לשם "שעשוע").
- "חבר" מקוון עשוי להתברר כמשהו אחר.
- ההערות שלך בפורום מפריעות למישהו שמחליט שעליו "ללמדך לקח".

אלה רק חלק מהתסריטים; אתה בודאי יכול לדמיין אחרים (וכן, דברים כאלה באמת קורים; ראה הערה מוצללת "האם באמת קורים דברים כאלה?" בהמשך פרק זה).

כדי לשמור על זהותך התייחס להנחיות הבאות:

1. אל תיתן את מספר הטלפון שלך, כתובת מגורים, כתובת מקום עבודה, מקום בילוי, או כל פרט מזהה אחר.
2. הימנע מלתת את שמך המלא בעולם המקוון, אף אם שם המשפחה שלך רגיל.
3. אל תיפגש עם מי שאתה יוצר עימו קשר דרך האינטרנט. במקרה של חברות טובה עם חבר וירטואלי חדש, אל תיתן מידע כמו היכן אתה עובד, קונה, מבלה, עושה ספורט וכדומה.
4. אם אתה יוצר קשר רומנטי, בדוק וברר ככל הניתן לפני פגישה פנים אל פנים. חפש אחרים ברשת המכירים את האדם ונסה לגלות כמה שיותר פרטים אודותיו. קח את הטלפון של האדם - לעולם אל תיתן את שלך! - והתקשר מטלפון ציבורי. ואם אתם כן נפגשים, היפגשו במקום ציבורי.
5. לבסוף, הייה ספקן! אל תאמין למה שאומרים לך, עד לקבלת הוכחות.

האם באמת קורים דברים כאלה? סיפורים קצרים עם לקח...

מעניין שאפילו התקשורת לא מצליחה להגזים במה שבאמת קורה באינטרנט. להלן טעימה קלה של מוזרויות:

- עשרות מקרים של אנשים שמציגים את עצמם באור שונה מהמציאות או פשוט משקרים ביחס לעצמם; עורך דין שהוא לא כזה, רופא, שחקן קולנוע, טייס, פסיכולוג ורבים אחרים.
- אישה שנענתה למודעה אישית מקוונות, פגשה בגבר, והחליטה שהוא לא הטיפוס שלה. לאחר מספר ימים האישה הגיעה הביתה ומצאה אותו מחזיק את בנה וחבר כבני ערובה (למרבה המזל, לסיפור זה יש סוף טוב).
- תלמיד התיכון שגנב כרטיס אשראי כדי לצפות באתרי פורנוגרפיה מקוונים. הוא חשב שהוא אלמוני ולעולם לא יתגלה - לבסוף הוא התגלה.
- מוכרים ש"נעלמים" לאחר שהציעו דברים למכירה במחירים נמוכים במיוחד, כאשר התשלום נדרש בצורה מקוונת או דרך תיבת דואר. הסחורה לעולם לא מגיעה, ואין דרך לאתר את הגנב.
- מקרים של גניבת זהות, כאשר אנשים המחפשים נקמה שלחו הודעות דואר אלקטרוני מזויפות, השאירו הודעות מזויפות בפורום, ואפילו תצלומים של קורבנותיהם.
- מבוגרים שטענו שהם נערים, נערים שטענו שהם מבוגרים, וגברים שטענו שהם נשים (עוד לא שמעתי על אישה שטענה שהיא גבר).

כרטיס האשראי ומספר החשבון שלך

יתכן שאתה משלם לשירות האינטרנט שלך באמצעות כרטיס אשראי. זה בסדר וכך משלמים רוב האנשים עבור שירות האינטרנט שלהם. לא סביר שמישהו יגנוב את נתוני כרטיס האשראי שלך בעת שהתחברת לראשונה. אולם, יש שיטות רבות להשגת נתוני כרטיס האשראי שלך ברשת, כמפורט להלן:

הגישה הנפוצה ביותר בידי גנבים, היא להציג עצמם בדואר אלקטרוני (או לעיתים בצ׳ט בזמן אמיתי) כעובדי אחד מספקי האינטרנט או שירות מקוון אחר, ושהם צריכים את פרטי כרטיס האשראי שלך ומועד הפקיעה לצורך אימות. או שיספרו לך שפרצו לחשבון שלך, או שיש בעיה אחרת כלשהי עם החשבון המקוון, ויבקשו את נתוני כרטיס האשראי שלך. ספקי אינטרנט ושירותים מקוונים מדגישים ש**לעולם** אינם עושים כך, ואף מזכירים זאת למשתמשיהם. לכן **לעולם אל תמסור את נתוני האשראי שלך בדואר אלקטרוני או בצ׳ט (Chat)** (ראה פרקים 1 ו- 8 למידע נוסף בנושא זה).

ככלל, קנייה מקוונת לרוב בטוחה - כאשר אתה קונה אצל סוחרים גדולים ומוכרים. למרות זאת, היו כמה מקרים בודדים שנעשה שימוש לרעה בנתוני כרטיס אשראי על ידי סוחרים מקוונים "קטנים".

היו גם מקרי הונאה באתרי אינטרנט ובדואר אלקטרוני בהם ה"סוחר" כביכול לוקח ממך מידע ואתה לעולם לא מקבל את הסחורה המוצעת. דבר דומה קורה במכירות פומביות מקוונות. או שאתה מקבל את הסחורה שהזמנת מעסק קטן, אך היא אינה כפי שפורסמה - ובשלב זה אתה עלול לגלות שהעסק נעלם.

השורה התחתונה היא זו: אל תיתן את נתוני כרטיס האשראי שלך לכל מי שמבקש והימנע מאתרים מפוקפקים, או כאלה המציעים משהו טוב מדי מכדי שיהיה אמת. אם העסק מתנהל באמצעות תיבת דואר, ואין מספר טלפון, דלג עליו.

בדומה, אל תמסור מספר חשבון בנק במערכת מקוונת, בדואר אלקטרוני או בכל דרך אחרת.

עצות לקנייה מקוונת

אם ניתן, השלם את הרכישה בדואר, בטלפון, או באופן אישי.

לעולם אל תיתן את מספר כרטיס האשראי שלך באתר לא מאובטח. אתרים המציעים מערכות מאובטחות מודיעים על כך. דפדפן האינטרנט אמור להודיע לך אם האתר מאובטח על ידי הצגת מנעול בשורת המצב. כמו כן, בשורת המצב הכתובת תתחיל ב-http**s** במקום http.

אבטחת מידע מקוון

ישנה דאגה רבה בין משתמשי אינטרנט בקשר לפגיעות של המידע המשודר. כידוע, מידע משודר דרך האינטרנט על ידי העברה בין מספר מחשבים. עקב כך, קיימת אפשרות שניתן יהיה לצפות במידע באחת מתחנות ממסר אלה. קשה לומר מה הסיכוי שדבר כזה יקרה, אך האפשרות קיימת.

ניתן לטפל בסכנה אפשרית זו במספר דרכים:

1. הימנע משליחת מידע רגיש דרך האינטרנט - כולל מספרי כרטיס אשראי. זה הגיוני, אף שמספר המקרים המדווחים של קליטת מידע באינטרנט ו"בילוש" אחר ודואר אלקטרוני באינטרנט הוא נמוך.
2. השתמש בתכונות האבטחה של הדפדפן והאינטרנט.
3. כדאי לשקול גם הצפנת מידע ודואר אלקטרוני רגישים (הצפנה נידונה בפירוט בפרק 7, ונדון בכך שוב בפרק 10).

תכונות אבטחה של דפדפנים והאינטרנט

תקני אבטחה עוסקים בהצפנת מידע, ובאבטחת המידע בעת שידור. ניצול תכונות אלו דורש שדפדפן האינטרנט שלך יתאים לתקני האבטחה שהם :

- Secure Socket Layer (SSL)
- Private Communication (PCT).

שני הדפדפנים Netscape ו-Internet Explorer תומכים בתקני אבטחה אלה.

חלק מתכונות האבטחה החשובות ביותר מובנות בתוך הדפדפנים. תכונות אלו כוללות **מסמכי אבטחה (Security Certificates)** לאימות זהותך באתר, אזהרות ש-Netscape ו-Internet explorer מציגות כאשר אתה מתחיל לשלוח נתונים לאתר אינטרנט לא מאובטח, ועוד. רצוי להשאיר תכונות אלו פעילות.

אתרי אינטרנט מספקים אבטחה אם הדפדפן שברשותך תומך בפרוטוקולים של אבטחה המשמשים באתרים אלה. תכונות אבטחה של אתרי אינטרנט כוללות מסמכי אבטחה, המאשרים שהם אכן כפי שהם טוענים, **אתרים מאובטחים**.

אתרים מאובטחים

אתר מאובטח מגן על התשדורות ממנו ואליו, כך שמספרי כרטיס אשראי ומידע רגיש אחר לא יוכלו להיקרא **בדרך** אליו. עדיין עליך לסמוך על בעלי האתר כמובן, אך זה כמו מסירת מספר כרטיס האשראי באמצעות הטלפון. אתרים מאובטחים מספקים מידת ביטחון שפרט לך ולאדם לו אתה מוסר מידע רגיש (בעלי האתר), לאיש לא יהיה את המידע.

בדיקת האבטחה

ישנן מספר דרכים לבדוק אם האתר בו אתה מבקר הוא אתר מאובטח. אם אתה משתמש ב-Netscape, לחץ על לחצן Security בסרגל הלחצנים (או על 🔒, המנעול בצד התחתון שמאלי של מסך Netscape). תופיע תיבת דו-שיח שתודיע לך איזה מהקבצים שדרשת הם מאובטחים, כמתואר בתרשים 9.1 (כאשר Netscape מקבל מסמך מאובטח, סמל המנעול מוצג סגור).



תרשים 9.1 בדיקת אבטחה עם Netscape

דפדפן Internet explorer של מיקרוסופט מעיד על תעבורת נתונים עם אתר מאובטח על ידי הצגת סמל הנראה כמו 🔒, מנעול בסרגל הסטטוס.

שני הדפדפנים יכולים להתריע על סכנת אבטחה, במצבים כגון שליחת מידע באמצעות טופס מקוון, שיכול להיות סיכון אבטחה. בדפדפן Netscape, בחר בתפריט **Options**, בחר בכרטיסיה **General**, כדי לאפשר או לבטל אזהרות על אתרים לא מאובטחים. בדפדפן Internet explorer, בחר **כלים**, לחץ על **אפשרויות אינטרנט**. בתפריט **כרטיסיה**, לחץ על לחצן **אבטחה**, ובחר ב**רמה מותאמת אישית**.

לבסוף, אם כתובת URL מתחילה עם https:// ולא עם http://, הכתובת היא בשרת מאובטח. בדומה, אם URL של פורום Newsnet מתחיל ב-:snews במקום ב-:news, הוא מאובטח.

אבטחת הורדה

כפי שנידון בפרק 8, הנזק הנגרם על ידי וירוסים וסוסים טרויאניים הוא רב ביותר, כך שעליך לשקול את המהות והמקור של כל הורדה מקוונת.

ככלל, עקוב אחר ההנחיות הבאות כדי להחליט מה להוריד:

- אם תוכנה או ערכת מאקרו מציעים תכונות בלתי אפשריות, או לפחות טובות מכדי להיות אמיתיות, דלג עליהם.
- אם אתר אינטרנט או שירות מקוון מדווח מעט או בכלל לא על בדיקות שעוברים הקבצים בו לגילוי וירוסים, אל תוריד משם קבצים.
- חפש הערות על הקובץ להורדה.
- לאחר שהורדת קובץ (ו/או בעת הורדתו), סרוק אותו לגילוי וירוסים (ראה פרק 8).

טשטוש עקבות מקוונות

באשר לבילוש אחר פעילותך המקוונת, עיקר האיום **אינו מהשירות המקוון** - אלא מאנשים המחטטים במחשב שלך. לכן, עליך לטשטש את עקבותיך המקוונות, תיוק הודעות וחומר אחר, והרישומים שנשמרים על ידי דפדפן האינטרנט שלך.

אבטחה לא-מקוונת של הורדות

מה שהורדת יכול להעיד לא מעט על פעילותך המקוונת. כדי למנוע ממישהו לראות מה הורדת, הקפד תמיד למחוק או לנקות יומני הורדה הנשמרים על ידי התוכנות בהן אתה משתמש (אם קיימים כאלה).

אם תוכנה שהורדת מגיעה בתוך ארכיב או ארכיב-פרישה-עצמי הכולל מספר קבצים, עליך למחוק קבצים אלה לאחר התקנת התוכנה האמורה. עליך גם למחוק את ההורדה המקורית, כמובן. כדי לפשט הליך זה, הורד תוכנות תמיד לאותה תיקיית הורדות. בעת פרישה והתקנת תוכנה, בצע את הפרישה לתיקיה בשם install\. כך יהיה קל לאתר ולמחוק את כל קבצי ההתקנה (יש תוכנות המוחקות בעצמן את קבצי ההתקנה שלהן, אך אל תסמוך על כך).

עבור קבצים שאינם תוכנות, הזז אותם מתיקיית ההורדות שלך סמוך ככל הניתן למועד הורדתם. מומלץ ליצור תיקיה מיוחדת (אולי בשם holding\) עבור קבצים כאלה (בתיקיה זו תוכל גם לאחסן תוכנות שאינך מתכוון להתקין מייד). דאג שתיקיה זו על תכולתה תהיה בלתי נראית (פרק 5 מפרט כיצד לעשות זאת), וכך תהיה מוגן בצורה סבירה.

לאבטחה נוספת, תוכל להצפין קבצים מאוחסנים כאלה (ראה פרק 7), או להשתמש ב-WinZip כדי לשמור אותם בקובץ ZIP מוגן סיסמה (ראה פרק 3).

איתור ומחיקת רישומי פעילות מקוונת

כידוע, קל לעקוב אחר ביקוריך באתרי אינטרנט - ואפילו אחר הקשות מקשים בודדות - בעזרת תוכנה מתאימה. אך ניתן להגיע לתוצאות דומות פשוט על ידי צפייה בקובץ ההיסטוריה של Netscape או Internet explorer. קבצים אלה מתעדים את אתרי האינטרנט בהם ביקרת, עד רמת כתובות URL, ואף את השאילתות או הכנסת נתונים אחרים. במצב מקוון, ניתן לפתוח כל דף ברישום על ידי לחיצה כפולה על ה-URL.

רשימת ההיסטוריה של Netscape

בחן זאת לבד. בדפדפן Netscape, לחץ **Ctrl+H**, או בחר ***היסטוריה*** **(History)** בתפריט. יוצג חלון המכיל כתובות URL ומידע על הכתובות, כמתואר בתרשים 9.2.

כדי למחוק פריטי היסטוריית Netscape אחד-אחד, האר את הפריט הרצוי ולחץ על מקש **Delete**, או לחץ על **Select** מתפריט **Edit**, ואז לחץ על **Delete**.

History

File Edit View Communicator Help

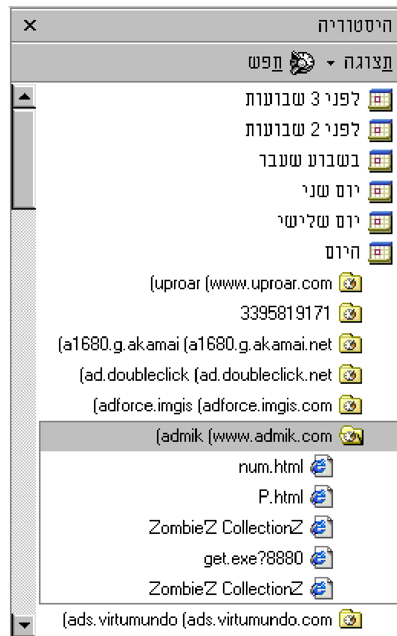
Title	Location	First Visited	Last Visited	Expiration	Visit Count
Welcome to NetChex	http://www.netchex.com/index.html	Less than one hour ...	Less than one hour...	1/13/2000 6:26 PM	1
Welcome to Sybex, Inc. - Quali...	http://www.sybex.com/	Less than one hour ...	Less than one hour...	1/13/2000 6:24 PM	1
Weather Underground: Louisvil...	http://www.wunderground.com/US...	9 hours ago	9 hours ago	1/13/2000 9:22 AM	1
RiverCon Science Fiction Conv...	http://members.aol.com/rivercon/	9 hours ago	9 hours ago	1/13/2000 9:19 AM	1
AltaVista Live	http://live.av.com/scripts/editorial.dl...	9 hours ago	9 hours ago	1/13/2000 9:16 AM	1
AltaVista - Search	http://www.altavista.com/	12/23/1999 1:16 PM	9 hours ago	1/13/2000 9:15 AM	21
McAfee.com - About McAfee.c...	http://www.mcafee.com/about/pre...	19 hours ago	19 hours ago	1/12/2000 11:11 PM	1
McAfee.com - The Place for Y...	http://www.mcafee.com/	12/26/1999 9:15 PM	19 hours ago	1/12/2000 11:07 PM	5
AltaVista - Web Results	http://www.altavista.com/cgi-bin/q...	1 days ago	1 days ago	1/12/2000 3:45 PM	1
Most of my MP3's	http://www.calpoly.edu/~mblackwo...	1 days ago	1 days ago	1/12/2000 3:43 PM	1
Error 404	http://frontpage.webzone.net/capta...	1 days ago	1 days ago	1/12/2000 3:43 PM	1
AltaVista - Web Results	http://www.altavista.com/cgi-bin/q...	1 days ago	1 days ago	1/12/2000 3:00 PM	1
Kevin's Wav Page	http://members.aol.com/Soundstuff...	1 days ago	1 days ago	1/12/2000 2:55 PM	1
AltaVista - Web Results	http://www.altavista.com/cgi-bin/q...	1 days ago	1 days ago	1/12/2000 2:54 PM	1
Airplane!: The Jive	http://www.iqtech.com/emrp/html/ji...	1 days ago	1 days ago	1/12/2000 2:49 PM	1
AltaVista - Web Results	http://www.altavista.com/cgi-bin/q...	1 days ago	1 days ago	1/12/2000 2:48 PM	1
AltaVista - Web Results	http://www.altavista.com/cgi-bin/q...	1 days ago	1 days ago	1/12/2000 2:47 PM	1
Zip2 Maps & Directions Map of ...	http://www.zip2.com/altavista/scrip...	2 days ago	2 days ago	1/11/2000 1:47 PM	1
Zip2 Maps & Directions	http://www.zip2.com/altavista/scrip...	2 days ago	2 days ago	1/11/2000 1:47 PM	1
Zip2 Maps & Directions	http://maps.altavista.com/	2 days ago	2 days ago	1/11/2000 1:47 PM	1
Not Found	http://maps.altavista.com/cgi-bin/m...	2 days ago	2 days ago	1/11/2000 1:47 PM	1
Snap.com	http://listen.snap.com/nullresults.jsp...	3 days ago	3 days ago	1/10/2000 10:11 PM	1
Search Results	http://listen.snap.com/results.jsp?ar...	3 days ago	3 days ago	1/10/2000 10:10 PM	1
Snap! Music Search	http://listen.snap.com/sub1.jsp?par...	3 days ago	3 days ago	1/10/2000 10:04 PM	1
Snap: Guide to Music Downloa...	http://real.snap.com/LMOID/resour...	3 days ago	3 days ago	1/10/2000 10:03 PM	1
Hottest MP3's on the Net	http://real.snap.com/flat/real_popu...	3 days ago	3 days ago	1/10/2000 10:02 PM	1
Snap: Search Results	http://real.snap.com/search/directo...	3 days ago	3 days ago	1/10/2000 10:02 PM	1
HotBot results: Pilot of the Airw...	http://hotbot.lycos.com/?MT=Pilot+...	3 days ago	3 days ago	1/10/2000 10:01 PM	1
Real.com - Guide - Search	http://realguide.real.com/search/?s...	3 days ago	3 days ago	1/10/2000 10:00 PM	1
HotBot	http://hotbot.lycos.com/	3 days ago	3 days ago	1/10/2000 9:59 PM	1
HGR Music Catalogue, Edition ...	http://www.hgr.co.uk/cd2.htm	3 days ago	3 days ago	1/10/2000 9:53 PM	1
PETE'S LOTTA' LINKS PAGE ...	http://www.geocities.com/Athens/...	3 days ago	3 days ago	1/10/2000 9:53 PM	2

Netscape

תרשים 9.2 רשימת ההיסטוריה של Netscape מספקת פירוט רב על פעילותך באינטרנט

רשימת ההיסטוריה של Internet explorer

היסטוריית URL של Internet explorer מאוחסנת בתיקיות לפי שבוע, ולפי אתרי אינטרנט, כמתואר בתרשים 9.3. לחיצה על לחצן **היסטוריה** בסרגל התפריטים מציג חלון קטן עם רשימת URL בהם ביקרת (ניתן גם לבחור את סרגל Internet explorer בתפריט **תצוגה**, ללחוץ על **היסטוריה**, או להקיש **Ctrl+H**).



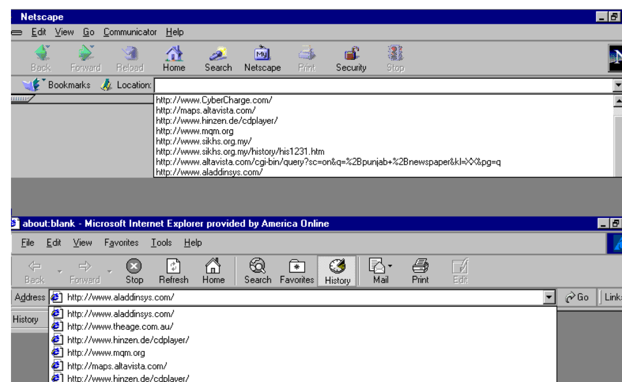
תרשים 9.3 רשימת ההיסטוריה של Internet explorer מספקת רשימות ממוינות של אתרי האינטרנט בהם ביקרת

ניתן למחוק URL בודדים, אך הדרך המהירה ביותר היא למחוק שבועות שלמים או תיקיות אתרי אינטרנט. או, ניתן לנקות את תיקיית ההיסטוריה לחלוטין על ידי בחירה בתפריט **כלים (tools)** של Internet explorer, לחיצה על **אפשרויות אינטרנט**, בחירה בכרטיסיה **כללי**, ואז לחיצה על לחצן **נקה היסטוריה**.

כניסה פרטית

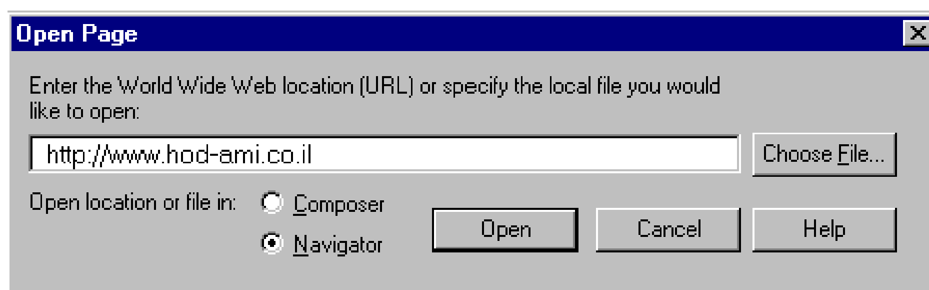
משתמשי אינטרנט נכנסים לעיתים לאתרים בצורה ידנית, על ידי הקלדת כתובת או הדבקתה. יש שתי דרכים לעשות זאת, האחת משאירה עקבות והשנייה לא.

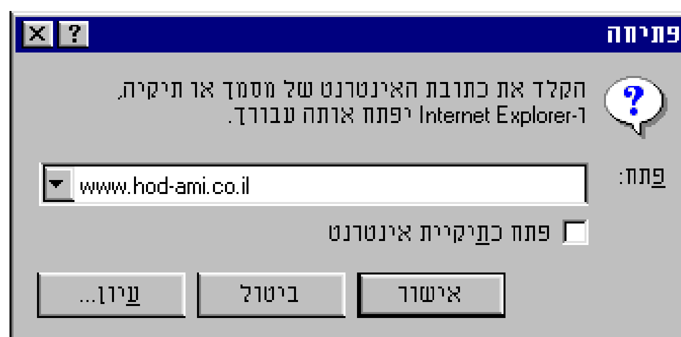
אם תכניס URL בסרגל המיקומים שמתחת לסרגל הכלים ב-Netscape או Internet explorer, ה-URL נרשם ברשימה הנגללת, כמתואר בתרשים 9.4 (גם URL שביקרת בו עקב פתיחת קישור בחלון חדש, נרשם).



תרשים 9.4 שדה המיקום של Netscape וסרגל ההכתובות של Internet explorer מספקים תיעוד היכן ביקרת באינטרנט

המידע נשאר שם עד שרישומים אחרים גורמים לו להימחק. כדי לפתוח דף בלי שכתובתו תירשם בשדה זה, בחר ב-Open Page בתפריט File של Netscape, או פתח תפריט קובץ של Internet explorer. הכנס את ה-URL בתיבת הדו-שיח (לחליפין, ניתן ללחוץ על **Ctrl+O** ב-Netscape וב-Internet explorer). תרשים 9.5 מציג את תיבות הדו-שיח של שני הדפדפנים.

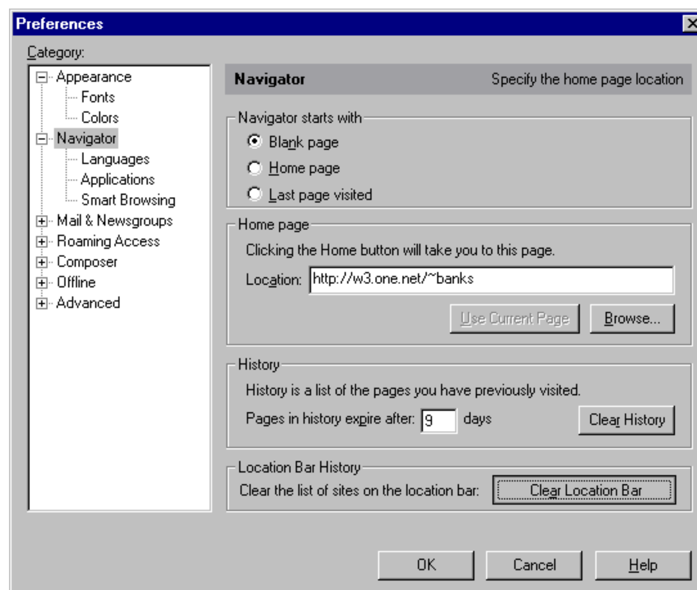




תרשים 9.5 הכנסת דף אינטרנט בצורה ידנית - ובדוגמאות ב-Netscape וב-Internet explorer

ניקוי שדה מיקום (Location Field) של Netscape

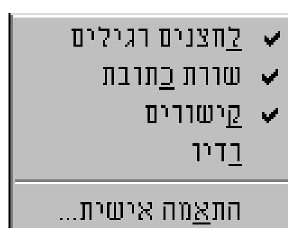
אם ברצונך להיפטר ממידע בשדה המיקום של Netscape, Netscape מאפשרת לך לנקותו. כדי לעשות כן, בתפריט **Edit** של Netscape, בחר **Preferences**, ולחץ על **Navigator**. תיבת הדו-שיח של **Preferences** תופיע, כמתואר בתרשים 9.6. לחץ על הלחצן **Clear Location Bar**, ורישומי ביקוריך באינטרנט ייעלמו.



תרשים 9.6 ניקוי שדה המיקומים של Netscape

הסתרת סרגל הכתובות של Internet explorer

ניתן להסתיר את שדה הכתובות של Internet explorer. לחץ לחיצה ימנית על סרגל הכלים והסר התיוג מתוויות **שורת כתובת (Address Bar)**, כמתואר בתרשים 9.7.



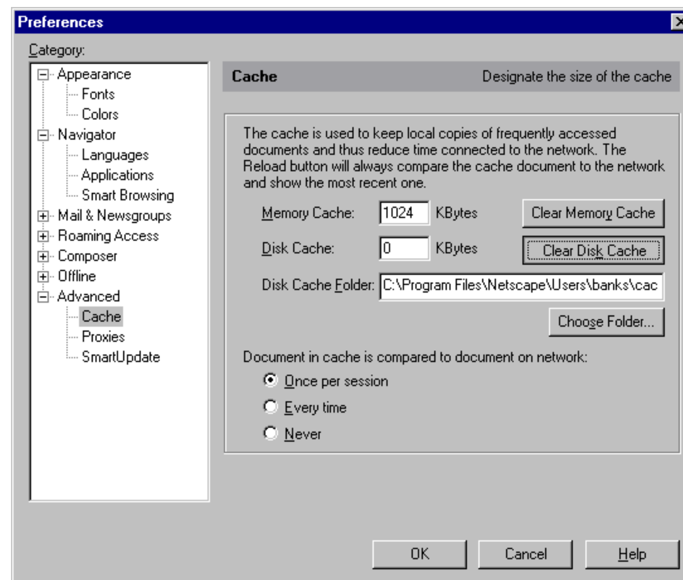
תרשים 9.7 הסתרת שורת הכתובת של Internet explorer

בדיקת זיכרון המטמון

Internet explorer ו-Netscape שומרים תמונות ודפי HTML אחרונים שביקרת בהם בזיכרון המטמון של הדיסק הקשיח. פעולה זו מאיצה גישה לאינטרנט עבור דפים שאתה חוזר ומבקר בהם, אולם, קבצים אלה נגישים לכל מי שיודע באילו תיקיות לחפש.

קבצים אלה מאוחסנים במספר תת תיקיות (מובן מאליו שגם בתיקיה Cache\), אך אינך צריך לדעת היכן הם כדי למחוק אותם. כל שעליך לעשות הוא לנקות את המטמון של הדיסק.

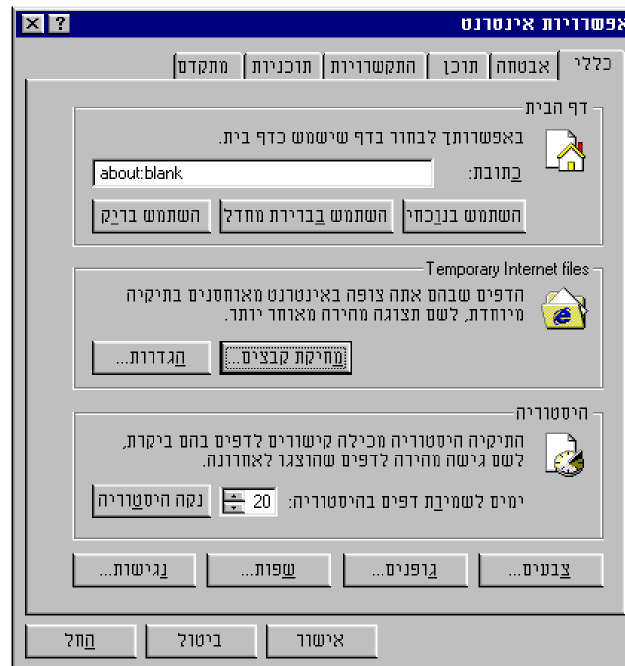
ב-Netscape, בתפריט **Edit**, בחר ב-**Preferences**. לחץ על + ליד **Advanced** **Selection**, ולחץ **Cache**. לחץ על לחצן האפשרויות בשם **Clear Disk Cache**, כמתואר בתרשים 9.8.



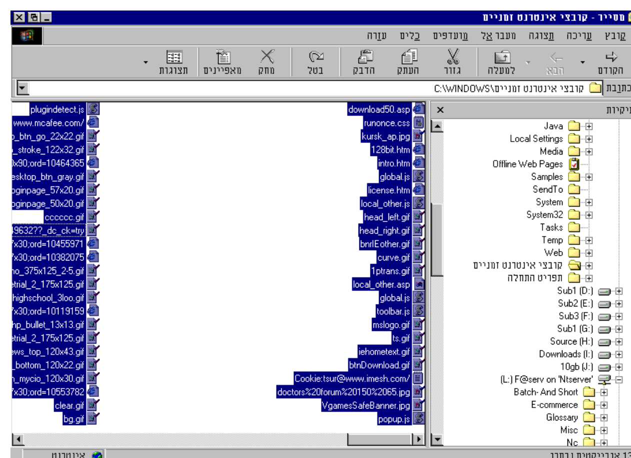
תרשים 9.8 ניקוי מטמון הדיסק ב-Netscape

ב-Internet explorer, בתפריט **תצוגה (View)**, בחר ב**אפשרויות אינטרנט (Internet) Options**, ולחץ על לחצן **כללי (General)**. לחץ על הלחצן **מחיקת קבצים (Delete Files)** כדי למחוק את הדפים ש-Internet explorer שמר (תרשים 9.9).

משתמשי Internet explorer יצטרכו גם לנקות תיקיה המשמשת לשמירת קבצי אינטרנט זמניים. הקובץ נמצא בתיקיית Windows על הדיסק הקשיח הראשי - לרוב כונן C. פתח את סייר Windows, ופתח את **C:\Windows\קבצי אינטרנט זמניים (C:\Windows\Temporary Internet Files)**, כמתואר בתרשים 9.10.



תרשים 9.9 ניקוי מטמון הדיסק של Internet explorer



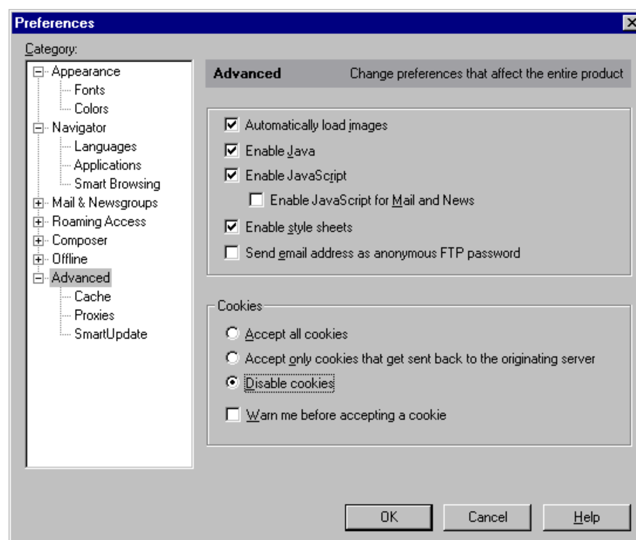
תרשים 9.10 ניקוי קבצי אינטרנט זמניים

פתח את תפריט **עריכה (Edit)** ולחץ **בחר הכל (Select All)**. עתה לחץ על מקש **מחק (Delete)**. רוב הקבצים בתיקיה יימחקו, כולל כמה קבצי Cookie שהוטמנו שם על ידי שרתי אינטרנט באתרים שביקרת בהם.

העלמת Cookies

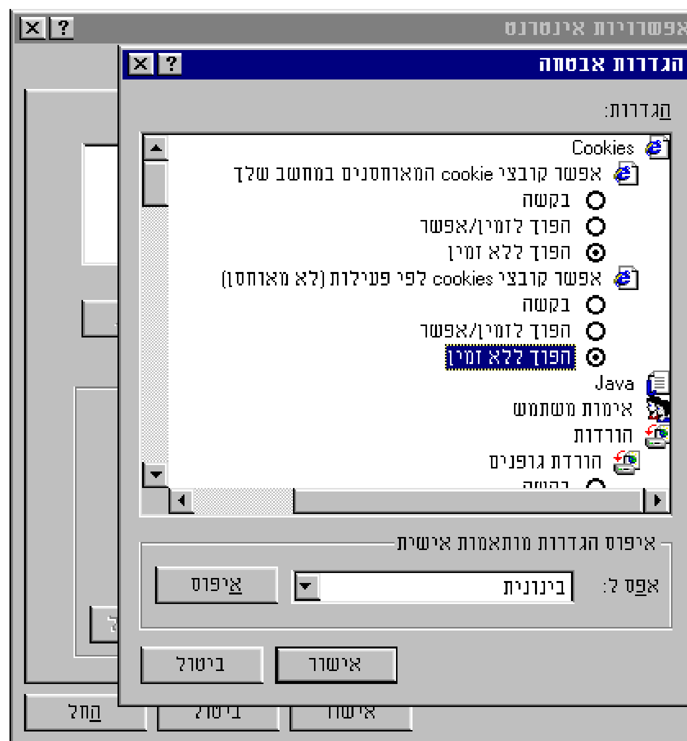
בהקשר ל-Cookies (אלה קבצים שהשרת אליו ניגשת רשם בדיסק שלך), עליך לדעת שאף שמחקת מטמוני דיסקים, קבצים אלה יישארו. בנוסף, כמתואר בתרשים 9.10, Cookies כוללים כתובות אתרי אינטרנט - ומכאן שכל אחד יכול לראות את כתובות האתרים בהם ביקרת. עדיף לבטל Cookies בדפדפן כדי למנוע שמירתם על הדיסק הקשיח.

לביטול Cookies עם Netscape, בתפריט **Edit**, לחץ על **Preferences**, בחר ב-**Advanced** ולחץ על לחצן האפשרויות **Disable Cookies** (תרשים 9.11).



תרשים 9.11 ביטול Cookies עם Netscape

לביטול Cookies ב-Internet explorer, בתפריט **כלים (Tools)**, בחר ב**אפשרויות אינטרנט (Internet Options)**, לחץ על **הגדרות אבטחה (Security)**, ולחץ על לחצן האפשרויות **רמת הגדרות מותאמות אישית (Custom Level)**. תיבת דו-שיח **הגדרות אבטחה (Security Settings)** תופיע, כמתואר בתרשים 9.12. בקבוצת ההגדרות **אפשר קבצי cookies לפי פעילות**, סמן את האפשרות **הפוך ללא זמין**, ובקבוצת ההגדרות **אפשר קבצי cookie המאוחסנים במחשב שלך**, סמן את האפשרות **הפוך ללא זמין**. לחץ אישור.



תרשים 9.12 ביטול Cookies עם Internet explorer

סימניות ורשימות מועדפים (Favorites)

הסימניות (Bookmarks/Favorites) שלך מספקות מידע רב על מעשיך המקוונים, כיון שאתרי אינטרנט בהם אתה מבקר תכופות, או אתרים מועדפים, נשמרים בקובץ הסימניות שלך. שקול ביטול סימניות אם יש חשש שהם יסגירו מידע שברצונך להסתיר.

פרק 10



הגנת דואר אלקטרוני

- דואר אלקטרוני ואיומי שווא על פרטיות
- סכנות מקוונות אמיתיות לדואר אלקטרוני
- כיצד דואר אלקטרוני מסכן אותך
- הצפנת דואר אלקטרוני ותוכנות הצפנה
- הגנת פרטיותך מדואר זבל (Spam)
- סכנות אמיתיות ולא מקוונות לדואר אלקטרוני
- תיוק דואר אלקטרוני והגנה על מערכת התיוק

פרטיות דואר אלקטרוני היא בין הנושאים החשובים ביותר אך הפחות מובנים באינטרנט. רבים מכם הקוראים ספר זה חוששים מאוד שאדם זר יקרא את הדואר האלקטרוני הפרטי שלכם. עקב כך, פרק זה יזהה את הסכנות לפרטיות דואר אלקטרוני וכיצד להגן על פרטיותך בעת שליחה, קבלה, ואחסון דואר אלקטרוני.

דואר אלקטרוני ואיומי שווא על פרטיותך

כמו משתמשי אינטרנט רבים, גם אתה אולי מודאג מאוד מכך שהדואר האלקטרוני שלך ייקלט וייקרא על ידי אחרים. למעשה, יש סבירות נמוכה מאוד שדבר כזה יקרה, כפי שיוסבר בסעיף הבא. מבחינתי, אני לא מודאג מקליטת הדואר האלקטרוני שלי, בעיקר כיון שאיני אומר דברים בהודעות דואר אלקטרוני שלא הייתי רוצה שייוודעו ברבים. באשר לשידור עצמו, השיקול היחיד שלי זה שההודעות יגיעו ליעדן. רוב הדואר האלקטרוני שאני כותב ישעמם אדם זר.

אולם, אם אתה חושש מקריאת הדואר האלקטרוני שלך על ידי אדם זר, הסעיף הבא יעניין אותך.

אם כך, האם ניתן לקלוט ("ליירט") את הדואר האלקטרוני שלי?

התשובה הפשוטה לשאלה בכותרת היא "כן". האם ניתן לקלוט את הדואר האלקטרוני שלי בקלות? התשובה הפשוטה הפעם היא "לא". בעיקרון, קליטת הודעות דואר אלקטרוני באינטרנט דורשת תכנון ומאמץ לא מבוטל.

נתונים - כולל דואר אלקטרוני - משודרים באינטרנט ב**מנות (Packets)**. המשמעות היא שדואר אלקטרוני נשלח בחלקים. כדי לסבך את העניינים, לא כל מנה נשלחת באותו נתיב וירטואלי. כך, כל מי שרוצה לקלוט את הדואר האלקטרוני שלך חייב להיות בעל מומחיות טכנית רבה בנוסף לגישה למחשבים ו/או קווי תקשורת נתונים המטפלים בדואר האלקטרוני שלך. פעולה זו מכונה לעיתים **Packet Sniffing**.

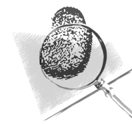
רצוי גם להבין שאם דברים שאתה רושם בדואר אלקטרוני נראים לך חשובים, פרטיים, רגישים או אינטנסיביים, הם כמעט שלא יעניינו אנשים אחרים. קריאת הדואר האלקטרוני שלך אולי תשעשע אדם כלשהו, אך לא יותר.

מה בנוגע למנהל המערכת (Sysop)? מה יכולים מנהלי מערכות לראות?

מנהלי מערכות - ואחרים עם הרשאות מתאימות - בספקי אינטרנט ושירותים מקוונים יכולים לראות אותך. למעשה, ניתן לראות ולתעד את כל מעשיך. או, כפי שמנהל מערכת פעם אמר לי "אנו יכולים לראות כל הקשה שתבצע".

כמובן, שכוח האדם או המנהלים לא יטריחו את עצמם להסתכל ללא סיבה טובה; הם עסוקים מדי.

השורה התחתונה היא שלא תוכל לעשות הרבה למנוע ממישהו בעמדה המתאימה לקלוט את הדואר האלקטרוני שלך. אולם, תוכל לשמור על פרטיות תוכן הדואר האלקטרוני, בטכניקות שיידונו בהמשך.



אם אתה עובד בחברה גדולה או קטנה, או במשרד ממשלתי, צא מתוך הנחה שהדואר האלקטרוני שלך נקרא. חוק Electronic Communications Privacy Act משנת 1986 (בארה"ב) מסיר אחריות מעובדים בקליטה וקריאת דואר אלקטרוני (שאחרת אינה חוקית). במילים אחרות, למעסיק שלך מותר על פי חוק לקרוא כל דואר אלקטרוני שאתה שולח או מקבל באמצעות מחשבי החברה.

סכנות מקוונות אמיתיות של דואר אלקטרוני

מעבר לכך שמישהו יתעניין מספיק כדי לטרוח, לקלוט, ולהרכיב את מנות הדואר האלקטרוני המקוונות שלך בדרכן, דואר אלקטרוני מציב שתי סכנות אמיתיות. סכנות אלו אינן כרוכות בקליטת הדואר האלקטרוני שלך, אלא באופן בו מתבצעת הקבלה והשליחה של דואר אלקטרוני.

חשיפה לא מוסרית?

הסכנה המקוונת הראשונה היא ברורה: נמען יכול להשתמש בדואר אלקטרוני פרטי ולהעביר מידע עליך או ממך לאחרים - ובלי ידיעתך. סביר להניח שאם תכתוב משהו מקוון משעשע, אחרים ישותפו בו.

כיון שקל מאוד להפנות דואר אלקטרוני הלאה (Forward), עליך לסמוך על הנמענים שלך או להימנע מהכנסת מידע חסוי לדואר אלקטרוני, ובמיוחד ביחס להודעות מביכות.

שמור על קור רוח

יש סכנה שמישהו ישתמש בדואר האלקטרוני שלך נגדך, בדיוק כמו בפורום (קבוצות דיון). אם יש לך נטייה להתפרצויות ולאמירת דברים חסרי טקט לאנשים שאינך מכיר (או לאנשים שאתה כן מכיר), עוד תגלה יום אחד שהודעותיך הופצו לאחרים.

אל תשלח Spam או Scam (שליחה למאות כתובות סתמיות, או שליחת דואר זבל)

אם תשלח Spam, אתה עוד עלול להגיע לרשימה השחורה באחד מאתרי האינטרנט מסוג זה. לא חשוב היכן תשלח Spam; תעורר שנאה בכל אתר באינטרנט. כך שאם אתה יזם צעיר המחפש להתעשר מהר על ידי משלוח הצעות למאות-אלפי "קונים" באינטרנט, עצור ושקול שנית.



אם תשלח הרבה דואר אלקטרוני לאנשים שאינך מכיר, רצוי שתעלים את שמך האמיתי מהכותרות. זאת כיון שאינך יודע כמה פעמים ולמי הודעה ששלחת תועתק ותישלח הלאה - בשוגג או בכוונה. גש לתפריטי **אפשרויות (Options)** או **Set Up** ומחק את שמך האישי. כך יש לך יותר שליטה לאן ומי יידע את שמך המלא.

מה הוא Spam

אם אתה מקוון מספר חודשים כבר בוודאי חווית זאת: אתה מתחבר כדי לבדוק את הדואר האלקטרוני שלך, ומגלה שיש לך הרבה דואר אלקטרוני חדש, וכולו מאנשים שאינך מכיר. כותרות הנושא מכריזות: "עשה כסף בעודך ישן", "תוכל להרוויח 1000 דולר בכל פעם שהטלפון מצלצל", או "צא לגמלאות בשבוע הבא!".

הצעות אלו נקראות Spam (השם נובע מסרט של מונטי פייטון בו קבוצת ויקינגים שרה "Spam, Spam, Spam, Spam" ומפריעה לסועד להזמין ארוחה. Spam הוא בערך ברמה כזו - מלל חסר ערך ללא כתובת). Spam מעמיס על מערכות דואר אלקטרוני, מציק לאנשים, וכמעט לעולם אינו מספק את הסחורה המוכרזת. חוסר יעילות זה נובע מכך שרוב ה-Spam מפרסם תוכניות פירמידה בלתי-חוקיות, או שיווק רב-שלבי כביכול או תוכניות שיווק שמעולם לא עובדות.

הכתובת הנכונה

הדרך השנייה להסתבך עם דואר אלקטרוני מקוון היא אופן הטיפול בדואר אלקטרוני, נכנס ויוצא. טעות אחת במיעון, ואתה מוצא את עצמך במצב מביך, או גרוע מזה.

כבר קיבלתי דואר אלקטרוני שלא היה מיועד לי. בין השאר היו שם תשובות לשאלות בנושאי עב״מים, תכתובת בין חברי קבוצה סודית של שירות מקוון שניסתה להכריח את ההנהלה לפטר מנהל מערכת, הזמנה לטקס, ומספר מכתבי אהבה שלא נועדו עבורי.

מוסר ההשכל מכל אלה. שים לב לכתובת אליה אתה שולח דואר אלקטרוני. אל תסמוך על רשימת הכתובות שלך או הזיכרון.

גם אני מיענתי דואר אלקטרוני לא נכון מספר פעמים - לרוב כי לא הייתי מרוכז והקלדתי את הדואר האלקטרוני של אדם כלשהו שחשבתי עליו באותו רגע, או ששלחתי לאדם אחר שזה עתה שלחתי לו דואר אלקטרוני, במקום לכתובת הנכונה. דרכים אחרות בהן אתה עלול להסתבך עם דואר אלקטרוני בעל מיעון שגוי הן:

- שליחת תשובה קבוצתית לכל אחד מחברי הקבוצה אליו נשלחה ההודעה המקורית. זה קורה כאשר אתה לוחץ על Reply All (מענה לכל) במקום פשוט Reply (מענה), כדי לתת תשובה להודעה שנשלחה אליך ולאחרים.
- קריאת הודעה שנשלחה אליך באמצעות Forward, ומענה לאדם ששלח - ולא לזה שכתב אותה לראשונה.
- שגיאה בכתיבת הכתובת עקב תווים דומים, ROGER או R0ger (עם אפס במקום האות O). אל תופתע אם הדואר ששלחת לא יגיע ליעדו...

האם הצפנה היא התשובה? (ואם לא, מה השאלה?)

כפי שניתן להבין, הדבר החשוב ביותר בנוגע לאבטחת דואר אלקטרוני הוא תשומת לב. הקפד על דבריך בדואר האלקטרוני הפרטי שלך, למי אתה שולח דואר אלקטרוני, ולאופן המיעון שלו.

מעבר להקפדה על מיעון הדואר האלקטרוני, רצוי להצפין דואר יוצא בעל אופי רגיש אם יש לך חשש כלשהו שמישהו יקלוט את הדואר בדרכו.

קח בחשבון שגם האדם בצד המקבל יכול לקלוט דואר אלקטרוני, אולי עמית לעבודה, חבר, או קרוב של הנמען. הצפנה תגן גם מבעיות מסוג זה.

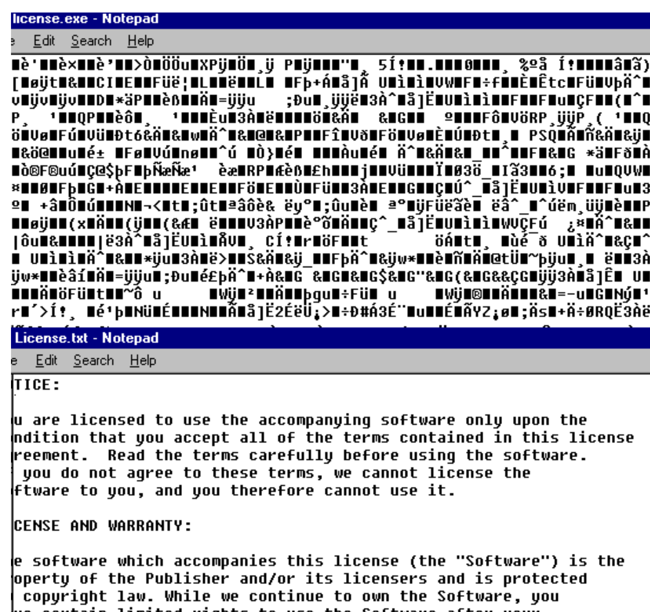
ביקור חוזר בתוכנות הצפנה

פרק 7 כולל דיון מעמיק על הצפנה, טכניקות הצפנה ותוכנות הצפנה. מומלץ להשתמש באחת מתוכנות ההצפנה הנידונות בו, ובין אלו, נראה ש-Norton Secret Stuff מציעה את השילוב הטוב ביותר של הצפנה וקלות שימוש ליישומי דואר אלקטרוני. כפי שצוין בפרק 7, Norton Secret Stuff יוצרת תוכנה המכילה הודעה מוצפנת או קובץ מוצפן אחר. התוכנה לא תריץ ותשחזר את הקובץ המוצפן ללא הסיסמה המתאימה.

תרשים 10.1, מציג כיצד נראה קובץ שהוצפן באמצעות Norton Secret Stuff. החלק העליון של התרשים מראה קטע מוצפן של הטקסט המופיע בחלק התחתון.

ברור שאין סיכוי רב שמישהו יוכל לקרוא את הקובץ בגירסה המוצפנת. וכיון שהתוכנה הכלולה בקובץ המוצפן לא תספק את הגירסה הלא-מוצפנת של הקובץ, אין לך מה לדאוג אם מישהו משיג עותק של ההודעה המוצפנת.

כמובן שתוכנות אחרות מציעות יתרונות אחרים. כפי שצוין בפרק 7, Pretty Good) PGP (Privacy מציעה חתימות דיגיטליות לאישור מסמכים של דואר אלקטרוני. זה יעניין את אלה מכם החוששים **מגניבת זהות** (גניבת זהות היא אדם המתחזה לאחר; זה עלול להיות בצורה של זיוף כתובתך בדואר האלקטרוני. חתימה דיגיטלית תמנע זאת - בנוסף לטכניקות אחרות).



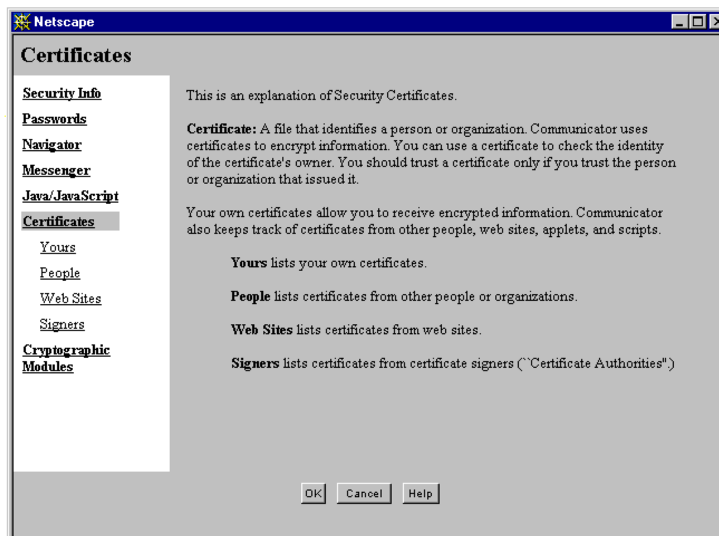
תרשים 10.1 הצפנה יוצרת טקסט שהוא בלתי קריא לחלוטין באמצעים מקובלים

תוכנות דואר אלקטרוני והצפנה

יש תוכנות דואר אלקטרוני המציעות הצפנה מובנית, כגון BeyondMail ו-Banyan (המיועדות בעיקר לשימוש ברשת), ו-Pegasus (המציעה תוסף תוכנה מותאם עבור PGP ותוכנות הצפנה מסוימות אחרות).

מערכת הדואר האלקטרוני של Netscape מאפשרת חתימה דיגיטלית על דואר יוצא באמצעות מערכת VeriSign הכלולה בדפדפן. כאפשרות, ניתן להצפין דואר למשתמש אחר אם יש ברשותו אישור דיגיטלי. נדרש לרכוש את האישור ולחדשו מדי שנה (ניתן לקבלו לתקופת ניסיון).

ניתן לקבל מידע נוסף על אישורים דיגיטליים ועל Netscape מדפדפן Netscape עצמו. לחץ על סמל **Lock** בצד השמאלי-תחתון של הדפדפן או מסך הדואר האלקטרוני; עתה לחץ על המילה **Certificates**. יופיע מסך כמתואר בתרשים 10.2.



תרשים 10.2 תיבת דו-שיח של Netscape עם מידע על אישורים

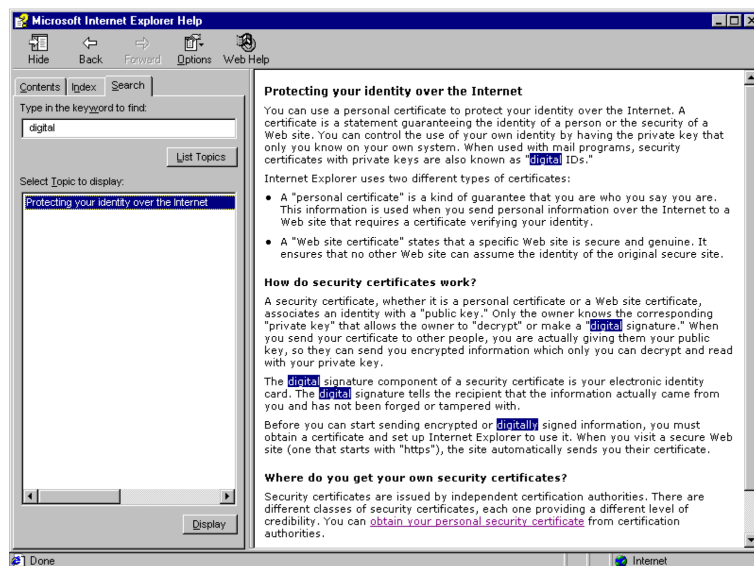
בחר באחת מן האפשרויות הבאות: **Yours**, **People**, **Web Sites**, **Signers** למידע מפורט.

Verisign גם מספקת אישורים דיגיטליים ל-Microsoft Outlook ו-Microsoft Outlook Express (למידע נוסף, בקר באתר VeriSign ב-http://www.verisign.com/).

גם Internet explorer מספקת הצפנה באמצעות אישור דיגיטלי של VeriSign (למשתמשי Internet explorer, יש שישה חודשי שירות חינם לשירות VeriSign). משתמשי Internet explorer יכולים גם לקבל אישור מ-GlobalSign בכתובת http://www.globalsign.net/products/.

Internet explorer מספקת מידע על אישורים דיגיטליים דרך מערכת העזרה. לחץ **תוכן (Contents)** ו**אינדקס (Index)** בתפריט העזרה של Internet explorer. הכנס **digital** בתיבת הטקסט, ולחץ על **רשימת נושאים (List Topics)**. תתקבל תיבת הדו-שיח כמתואר בתרשים 10.3.

כדי לקרוא על אישורים דיגיטליים, לחץ **הגנה על זהותך באינטרנט (Protecting Your Identity Over The Internet)**.



תרשים 10.3 עזרה של Internet explorer עם אישור דיגיטלי

הגנת הפרטיות מ-Spam

אולי אינך מודע לכך, אך כתובת הדואר האלקטרוני שלך היא נכס פרטי יקר ערך. היא גם מוצר בעל ערך לשולחי Spam ואחרים המעוניינים לפגוע בפרטיותך באמצעות הודעות פולשניות ולעיתים טורדניות, של הונאות, תעתועים, פורנוגרפיה וכדומה.

מבלי שניכנס לכל מיגוון ה-Spam הקיים ולדרכי ההסוואה השונות שלו על ידי יוצריו, היה בטוח שאינך רוצה שהדואר האלקטרוני שלך יגיע לשולחי Spam למיניהם. ניתן למנוע זאת באמצעות שמירה על כמה הוראות פשוטות כמתואר בסעיפים הבאים.

פתח כתובת דואר אלקטרוני חליפית

אל תציג את כתובת הדואר האלקטרוני שלך לציבור. אל תדוור במקומות ציבוריים באמצעות כתובתך, וכן אל תשתמש בה להירשם לחדרי צ'ט. אם אתה מתכוון לדוור במקומות ציבוריים, או להשתמש בחדרי צ'ט, השג כתובת חליפית למטרות אלו בלבד, ואל תטרח לבדוק בה דואר אלקטרוני נכנס.

שמור את הדואר האלקטרוני הראשי שלך לתכתובת עם חברים, קרובים או עמיתים עסקיים, כנדרש.

השגת כתובת חליפית אינה בעיה. אם אינך רוצה לרכוש חשבון נוסף אצל ספק אינטרנט, תוכל לקבל דואר אלקטרוני חינם במספר אתרים, וביניהם:

AltaVista: http://altavista.com

Exite Mail: http://mail.exite.com

Hotmail: http://www.hotmail.com

Net@address: http://netaddress.com

הקפד לא להיכלל ברשימות

שמור שכתובת הדואר האלקטרוני הראשית שלך לא תיכלל ברשימה כלשהי. אל תירשם לעדכונים באתר אינטרנט, והימנע מקבוצות דיון באמצעות דואר אלקטרוני, אלא אם אתה משתמש בכתובת דואר אלקטרוני חליפית או מבוססת אינטרנט.

שמור על פרופיל נמוך על ידי אי יצירת פרופיל

שירותים מקוונים, אתרי אינטרנט, וספקי אינטרנט רבים מספקים אמצעים מקוונים בהם ניתן לרשום מידע על עצמך - תחומי עניין, מקום, וכן הלאה. אמצעים אלה נקראים **פרופילים (Profiles)**. הפרופילים זמינים לכל מי שחפץ לעיין בהם, ושולחי Spam משתמשים בפרופילים מקוונים לעיתים תכופות כדי להוסיף אותם לרשימות הדיוור שלהם. אם יש לך פרופיל, מחק אותו; אם אין לך, אל תיצור פרופיל.

סכנות אמיתיות ולא מקוונות של דואר אלקטרוני

במצב לא-מקוון, הדאגה היחידה שלך היא שמישהו יעבור על הדואר האלקטרוני שלך ו/או ימחק הודעות. לכן יש לשקול כיצד להגן על הודעות שקיבלת ושמרת. ישנן מספר אפשרויות להגן על הדואר האלקטרוני מעיני אחרים ומהרס.

- הגן על הקבצים בתיבות הדואר הנכנס והיוצא (Inbox ו-Outbox) באמצעות סיסמאות.
- הצפן את תוכנת הדואר האלקטרוני ואת הקבצים.
- הדפס ושמור העתקים מודפסים.
- העתק הודעות רגישות שברצונך לשמור למעבד תמלילים והגן על הקבצים באמצעות סיסמאות ו/או הצפנה. אחסן אותם על דיסקטים או תקליטורים.

הצפנה היא ההגנה הטובה ביותר לדואר אלקטרוני. ניתן להגן על דואר אלקטרוני באמצעות הגדרות הסיסמה של התוכנה שלך, אך כפי שציינתי קודם יש דרכים לעקוף סיסמאות (מישהו שמכיר אותך עלול לנחש את הסיסמה; או, כל אדם בעל גישה לקבצי הדואר יכול לעיין בהן באמצעות מעבד תמלילים או תוכנה אחרת). הדפסה ושמירת העתקים מקלה מאוד על איתור מה שאתה מנסה להסתיר. אין הגנת סיסמאות או הצפנה להעתקים מודפסים -צריך רק שמישהו ימצא את התדפיסים.

לכן, רצוי להצפין את תוכנת הדואר האלקטרוני וקבציה על הדיסק הקשיח. מומלץ להשתמש בתוכנות Encrypted Magic Folders, Private File, או SecurePC בסדר הזה. לחליפין, תוכל לארוז את כל ההודעות שברצונך לשמור לסדרת קבצי מעבד תמלילים - כאשר כל קובץ מוגן על ידי הצפנה. לפעולה זו מומלץ להשתמש ב-Norton Secret Stuff או ב-Private File (שוב, ראה פרק 7), ואחסון על דיסקטים.

אלה הם הדברים בנוגע לאבטחה ולשמירת פרטיות הדואר האלקטרוני. עתה נעשה עוד מסע אחד לאינטרנט ונבחן תוכנות הגנה מבוססות-אינטרנט בפרק 11. תוכנות אלו נועדו להגן על פרטיותך המקוונת והבלתי-מקוונת.

פרק 11



ביקור חוזר באינטרנט: תוכנות עזר

- Cookies - מה הם וכיצד לנהל אותם
- גלישה אנונימית עם שרת Proxy
- עזרי תוכנה לפרטיות מקוונת ולא-מקוונת
- מספר מילים על תוכנות ניטור אינטרנט

פרק זה דן במספר מרכיבים נוספים של אבטחה ופרטיות בעת גלישה באינטרנט. תחילה נבחן מקרוב Cookies, העמוסים ביותר מידע אישי משחשבת.

לאחר מכן נבחן כיצד לגלוש באופן אנונימי בעזרת **Proxy Server**. מכאן נעבור לבחון מספר תוכנות שימושיות לטשטוש עקבותיך כאשר אינך מקוון, והגנה בעת שאתה מקוון.

לבסוף נעסוק בתוכנות ניטור - מן הסוג המדווח כמעט על כל דבר שאתה מקליד, כולל סיסמאות. נבחן את יכולתן והיכן לאתרן.

Cookies (עוגיות)

דנו בקצרה ב-Cookies בפרק 9. כאן נבחן אותם לעומק, כיצד הם נרשמו על המחשב שלך וכיצד לנהל אותן.

מה הם Cookies ומדוע הם נמצאים בדיסק הקשיח?

Cookie (עוגיה) הוא שורת מידע ששרת אינטרנט רושם בקובץ על הדיסק הקשיח שלך. השרת עושה זאת באמצעות דפדפן האינטרנט שלך. ככלל, Cookies מורכבים משורת מידע אחת. הם מאוחסנים בקובץ בשם cookies.txt באחת מתת-התיקיות של הדפדפן.

Cookies משמשים שרתי אינטרנט (המחשבים המארחים את אתרי האינטרנט) כאמצעי להניח מידע על הדיסק הקשיח שלך. סוג המידע המאוחסן ב-Cookies יכול לכלול, בין השאר, זיהוי משתמש (User ID) וסיסמאות, תאריכים ושעות ביקור באתר, דפים שניצפו, ומידע רב נוסף (בהתאם למה שהחליט מתכנת האתר).

יישומי Cookies מסוימים מועילים למבקר באתר. לדוגמה, זיהוי משתמש וסיסמה המאוחסנים ב-Cookies יכניסו אותך לאתר הדורש מידע זה ללא שתצטרך להקלידו כל פעם מחדש. Cookies גם יכולים להכיל רשימת העדפות לאתר אינטרנט וכך להתאים את תצוגת המידע באופן אישי. Cookies משמשים גם לשמירת פריטים בעגלות קניות וירטואליות (אם ביקרת פעם באתר קניות, הזמנת פריטים ועזבת בלי שהשלמת את הזמנתך וחזרת מאוחר יותר, ראית שרשימת הפריטים שלך נשארה שלמה. דבר זה בוצע על ידי קובץ Cookie ששחזר וחולל מחדש את רשימת הקניות). כמו כן, קבצים אלה עשויים לאחסן תיעוד באיזה דפים ביקרת באתר, מה חיפשת, ולהשתמש במידע זה כדי להנחות את השרת לאפשר גישה לדפים חדשים ולמנוע גישה לדפים בהם ביקרת בעבר. סידור כזה יכול להתאים לאיסוף ואחסון נתוני סקרים, תוך שהוא מונע ממישהו לבצע את הסקר פעמיים.

קובץ cookies.txt מוצג בפני כל שרת הדורש זאת. אולם, חלק ניכר מהמידע ב-Cookie שמיש רק לשרת שהניח את ה-Cookie, או לשרתים אחרים אשר כותב ה-Cookie בוחר לשתף.

הקובץ cookie.txt הוא קובץ ASCII הנראה בערך כך :

```
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file!  Do not edit.
.amazon.com TRUE    /    FALSE    2082787568  x-main  nIDfTAYzJDky5V6rp9
K6UZsS915ULEq4
.amazon.com TRUE    /    FALSE    2082787240  ubid-main     077-2649831-7662731
```

```
.egreetings.com TRUE / FALSE 1589544039 E-greetings
zRH-NpVWp3-ZNbT11-hcK3-1-zvWOx3
.excite.com TRUE / FALSE 1609415891 popup no
.egreetings.com TRUE / FALSE 2114510439 EGNauto 234719635
.amazon.de TRUE / FALSE 2082754840 x-acbde eKQIfwnxuF
7qtmM40x6VWAXh@Ih6Uo5H
www.shopping.com FALSE /store FALSE 969519639 ShopperID
B0C9PRNHEQS12LRS001PQJH9C0U246UE
www.jcpenney.com FALSE /jcp FALSE 1262325962 ShopperManager%2Fjcp
SHOPPERMANAGER%2FJCP=11BV2LKPSMUSH2GVH
00J74GDH2G9H9EP0e82KcKCZaZ0e82KcKCZaZT200BF9459B4BB67241C1FB9C5
06B605E751F
banner.freeservers.com FALSE /r/ FALSE 953737814 CTEST true
banner.freeservers.com FALSE /r/ FALSE 953737815 FSVIS_L 1999-09-24
banner.freeservers.com FALSE /r/ FALSE 953737815 FSVIS 1999-09
.usatoday.com TRUE / FALSE 978307117 RMID d132656538907180
.aaddzz.com TRUE / FALSE 94968486 ALTEMP|38284635|3891D0450055A86D
support.microsoft.com TRUE / FALSE 978249519 Params
S=F&HSL=0&FR=0&A=T&SD=GN&PSL=0&SPR=CHS&T=B&DU=C&T1=7d&TSL=0&FSL=
0&LN=EN%2DUS&SG=&SU
ad1.impulsebuy.net FALSE / FALSE 1072914778 IASIDX
949250012-1421663-192.168.0.42
www.missingmoney.com FALSE / FALSE 2137622210 CFTOKEN 90066
```



שים לב למשפט "Do not edit" (אל תערוך), סמוך לתחילת הקובץ. עריכת הקובץ הופכת אותו לחסר ערך. אם קובץ ה-Cookie משמש לשמירת סיסמאות ולמידע נוסף הנוגע לשימושך באתר האינטרנט - ממש לא רצוי לערוך קובץ זה. אם תערוך, שרתים באתר האמור לא יוכלו לקרוא את המידע השמור בקובץ ה-Cookie, ולכן לא יזהו אותך בעת שתבקר באתר כמשתמש שכבר ביקר באתר, אלא כגולש חדש באתר. כפי שוודאי הסקת, cookies.txt מכיל מידע היכן היית. לכן, ניתן למחוק את קובץ cookies.txt לחלוטין, פן חטטן כלשהו יחליט לעיין בקובץ זה.

דוגמה זו היא חלק קטן של קובץ cookies.txt בתיקיית Netscape. ה-Cookie עצמו הוא שורת המידע הבאה אחרי כתובת URL של כל שרת המופיע בקובץ (שים לב ששרת יכול להניח יותר מ-Cookie אחד בקובץ cookies.txt).

המידע הבא אחרי כל URL הוא חסר משמעות ברובו, והוא משמש את תוכנות איסוף המידע השוכנות בשרתים של אתרי אינטרנט (וכפי שנאמר קודם, עבור שרתים אחרים היכולים לשתף מידע שהונח על ידי השרתים האמורים).

אולם, משמעות חלק מן המידע, כגון זיהוי משתמשים וסיסמאות כניסה לאתרים, ברורה. חלק מהרישומים כוללים כתובות רשת של ספקי אינטרנט ששימשו אותך לביקור באתרים אלה. אחרים, הם עבור שרתים אליהם לא התחברת באופן ישיר, אלא שהאתר בו ביקרת התקשר אליהם בכדי להציג מידע המגיע מהם, באתר (השורה עבור ad1.impulsebuy.net היא דוגמה לכך. היא גרמה לכך שפרסומת תוצג בדף בו ביקרת, ותיעדה מידע על ביקורך ועל הפרסומת שהוצגה בפניך).

שאר הנתונים מוצפנים עם מחרוזות אותיות וספרות שהן בעלות משמעות לאתרים שהניחו אותן שם, או שהם מתייחסים לרכיבים או הגדרות ייחודיות לאתר נתון. לדוגמה, מחרוזות False\True (שקר/אמת), עשויה לציין אם המבקר כבר היה באתר בעבר ויש לו זיהוי (ID) באתר.

Cookies והמידע האישי שלך

ישנם שימושים אחרים ומגוונים ל-Cookies. יישומים שאינם מובנים מאליהם, הם איסוף נתונים **אודות** מבקרי אתר אינטרנט - לצורך סטטיסטיקות שיווק או תמיכה בתעריפי הפרסום של אתר אינטרנט מסחרי. סוג זה של מידע, הכולל נתונים דמוגרפיים בנוסף למידע על אילו פרסומות ראה המבקר, לאילו דפים ניגש, מהם המוצרים שהזמין, ובאיזה אתרים אחרים ביקר, נקרא **יצירת פרופיל (Profiling).** האיסוף הוא לרוב אנונימי - אך לא תמיד, כפי שנראה. חוקיותו מוטלת בספק.

יצירת פרופיל מידע מורכב ממה שמכונה מידע-בלתי-ניתן-לזיהוי-אישי. הוא עשוי לכלול את כתובת ספק האינטרנט שלך (כדי לאתר בדיוק היכן אתה גר), האם אתה משתמש באתר מסחרי, חינוכי או ממשלתי כדי לגשת לאינטרנט (edu ,com, או gov, בהתאמה), סוג המחשב והדפדפן המשמשים אותך, וכיצד אתה ניגש ומשתמש בדפים באתר.

כל עוד לא אכפת לך לספק מידע באופן חופשי על הרגליך באתר אינטרנט מסוים, לשרת של האתר, לא יתעוררו בעיות עם Cookies. אם, לעומת זאת, אתה חש שאגירת מידע אישי במחשב שלך ואחזור מידע זה לשימוש בעת ביקור חוזר באתר אינטרנט היא חדירה לפרטיות, התיאבון שלך לעוגיות (Cookies) מידע הוא בוודאי מזערי.

יש להניח שגם לא ימצא חן בעיניך שאתרי אינטרנט סוחרים ב-Cookies. וזה אכן קורה. בנוסף, אם סיפקת מידע אישי (שם, כתובת, מספר טלפון) באתר אחד, אתרים אחרים עלולים לשתף מידע זה - כולל מידע על מה ראית ועשית באתר האמור (דוגמה לכך מופיעה בהערה הבאה, בשם "המקרה של דפי אינטרנט שיצרו פרופילים").

אם אינך רוצה ש-Cookies ירוצו במערכת שלך ללא שליטה מסיבה כלשהי, שקול חסימתם או בקרה עליהם. ישנן מספר אפשרויות לקבוע אילו אתרים יוכלו לכתוב Cookies במערכת שלך - או לקרוא אותם. ישנן טכניקות עשה-זאת-בעצמך שיחסמו או יגבילו Cookies, וישנן תוכנות העושות זאת עבורך. פרטים על כך יבואו בהמשך.

המקרה של דפי אינטרנט שיצרו פרופילים

בעוד שכל אוהדי השיווק המקוון נשבעים שאיש לא אוסף ומשתף מידע אישי אודות צרכנים המבקרים באתרי אינטרנט, לאלפי גולשים אכן המידע האישי נפרץ ושותף.

בתחילת שנת 2000, התברר שאתרים מסוימים שדרשו ממבקרים מידע אישי, כגון השם האמיתי של המבקר, כתובת, ומספר טלפון (למטרת ביצוע הזמנות מסוחרים מקוונים) שיתפו מידע זה עם אתרים אחרים. המטרה? זיהוי גולשי אינטרנט בעת שביקרו באתרים אחרים בהם המידע האישי שותף.

על פי הסיפור שיצא לאור בעיתון USA Today, מתאם פרסומות אינטרנט גדול, בשם DoubleClick שיתף לא רק מידע דמוגרפי כללי על גולשים המבקרים באתרי לקוחותיו, אלא גם מידע אישי יותר, כגון שמות, כתובות, ומספרי טלפון.

בעקבות חדשות אלו, DoubleClick הכריזה שתאפשר לגולשים שהמידע הפרטי שלהם שותף, לבחור שלא לעשות כן ולצאת מהמערכת.

זו דוגמה אחת בלבד כיצד מידע שהוא כללי ואינו אישי באינטרנט, הופך למידע המאפשר זיהוי בקלות. כמה אתרים נוספים עושים זאת? אין כל דרך לדעת. אך יש דרך להפסיק זאת בצד שלך: ביטול Cookies - או לפחות להיות בררן איזה Cookies אתה מאפשר לדפדפן שלך לקבל.

חיתוך עוגיות עשה-זאת-בעצמך

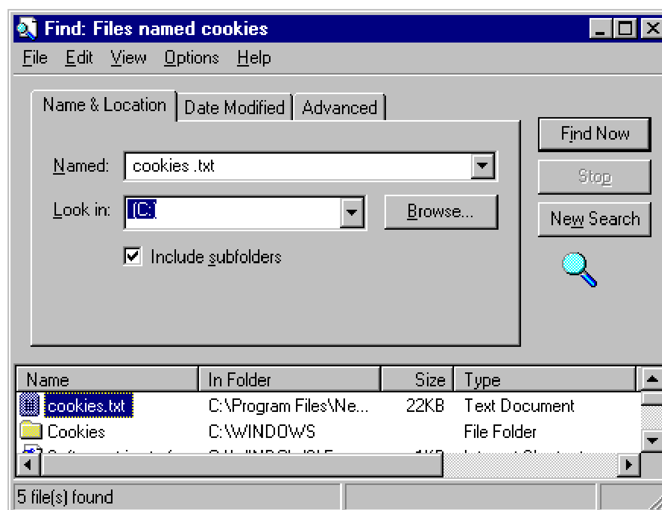
יש שתי גישות לעצירה או חסימה של Cookies. אחת היא ישירה וכרוכה במחיקת הקובץ cookies.txt. השנייה נעזרת באמצעים המסופקים על ידי Netscape ו-Internet explorer לעצירה או בקרה על Cookies.

למחוק את הקובץ?

גישה אחת לטיפול ב-Cookies היא למחוק או לערוך את הקובץ cookies.txt שהדפדפן רושם בדיסק הקשיח. אם בחרת בדרך זו, תדע שיהיה עליך לחזור ולמחוק את הקובץ. איני ממליץ על כך כיון שזו פעולה הגוזלת זמן רב, לאחר כל גלישה באינטרנט.

אולם, אם עדיין ברצונך למחוק Cookies - או רק להציץ בתכולתם - זו היא פעולה פשוטה. בהתאם להגדרות המחשב שלך והדפדפן בו אתה משתמש, קובץ זה יימצא באחת מכמה תיקיות; כך שקודם עליך לאתרו.

כדי למצוא את cookies.txt, השתמש ביכולות החיפוש של המערכת. בתפריט **התחלה** לחץ על **חפש**, ובחר ב**קבצים או תיקיות**. בתיבת הדו-שיח **חיפוש: כל הקבצים**, כמתואר בתרשים 11.1. הקלד **cookies.txt** ולחץ **חפש כעת**, או הקש **Enter**. ניתן לצפות בקובץ או למחוק אותו באמצעות תיבת דו-שיח זו בתפריט המופיע לאחר לחיצה ימנית עליו.



תרשים 11.1 השתמש בפעולת החיפוש של Windows לאיתור קובץ cookies.txt

חסימת גישה של Cookies בעזרת הגדרות דפדפן

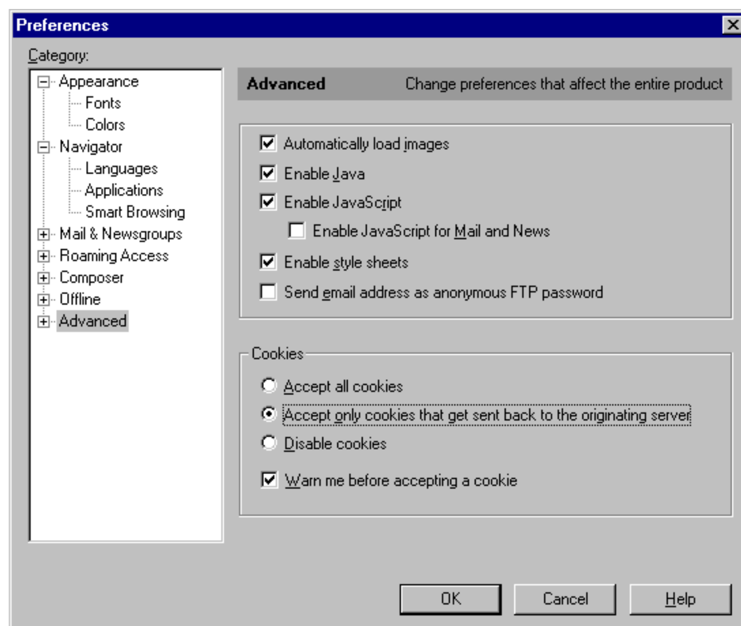
כפי שהוסבר ותואר בפרק 9, ניתן לחסום Cookies לחלוטין מהדיסק הקשיח, בעזרת ההגדרות של Netscape או Internet explorer, כדלקמן:

- ב-Netscape, בתפריט **Edit**, בחר ב-**Preferences**, לחץ על **Advanced**; עתה לחץ על לחצן האפשרויות **Disable Cookies** (תרשים 11.2).
- ב-Internet explorer גירסה 4, בתפריט **תצוגה (View)**, לחץ על **אפשרויות אינטרנט (Internet Options)**, ובחר בכרטיסיה **מתקדם (Advanced)**. השתמש בלחצן האפשרויות עבור **Cookies**.
- ב-Internet explorer גירסה 5, בתפריט **כלים (Tools)**, לחץ על **אפשרויות אינטרנט (Internet Options)**, בחר בכרטיסיה **אבטחה (Security)**, ולחץ על לחצן **רמה מותאמת אישית (Custom Level)**. (ראה תרשים 11.3).

בקרה על Cookies באמצעות הגדרות דפדפן

בנוסף לחסימה פשוטה של Cookies, ניתן להשתמש בהגדרות הדפדפן להגדרת רמות בקרה שונות של Cookies.

להלן הדרך לעשות זאת עם Netscape, בתפריט **Edit**, לחץ על **Preferences**, ובחר ב-**Advanced**; תיבת הדו-שיח **Preferences** תופיע, כמתואר בתרשים 11.2.



תרשים 11.2 תיבת הדו-שיח Preferences (העדפות)

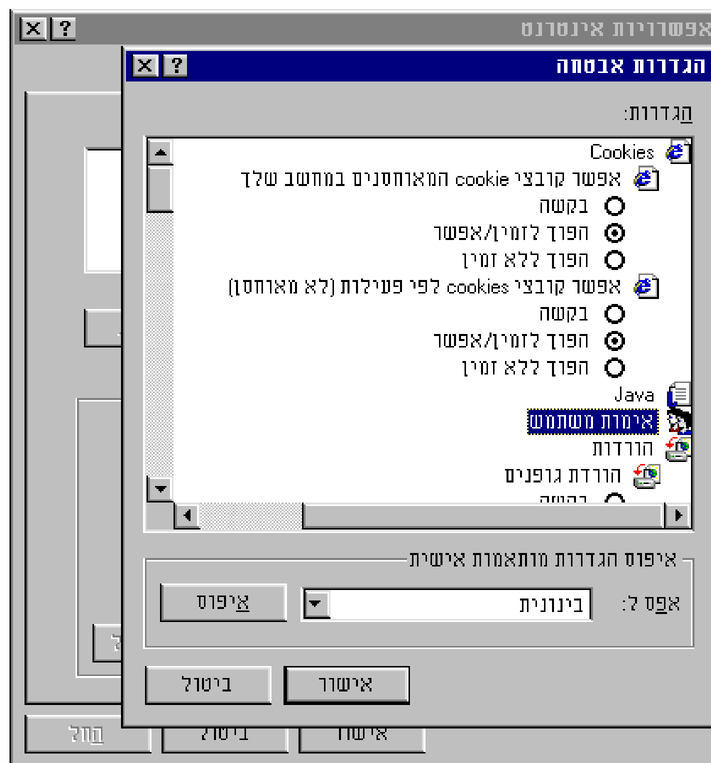
כפי שאתה רואה, בנוסף לחסימת Cookies, תיבת דו-שיח זו גם מאפשרת:

- לקבל את כל ה-Cookies.
- לקבל רק Cookies הנשלחים חזרה לשרת המקור שלהם, וזה מונע שפרטי מידע על ביקורך באתר אחד יעברו מייד לאתר אחר.
- לא לאפשר Cookies.

שים לב שיהיה עליך לבחור אחת מבין 3 האפשרויות הראשונות, וללא קשר למה שבחרת לעיל, תוכל לבחור או לא לבחור את הצגת האזהרה הבאה.

- לקבל אזהרה לפני אישור Cookies, המאפשרת לך לבחור אם Cookie ייכתב לדיסק הקשיח. בין אם הגדרת לקבל את כל ה-Cookies או לקבל רק את אלה הנשלחים חזרה לשרת המקור שלהם.

להלן הדרך לגשת להגדרות Cookies של Internet explorer בגירסה 5, בתפריט **כלים (Tools)**, לחץ על **אפשרויות אינטרנט (Internet Options)**, בחר בכרטיסיה **אבטחה (Security)**, ולחץ על לחצן **רמה מותאמת אישית (Custom Level)**, להצגת תיבת הדו-שיח **הגדרות אבטחה (Security Settings)** כמתואר בתרשים 11.3.



תרשים 11.3 בקרת Cookies של Internet explorer

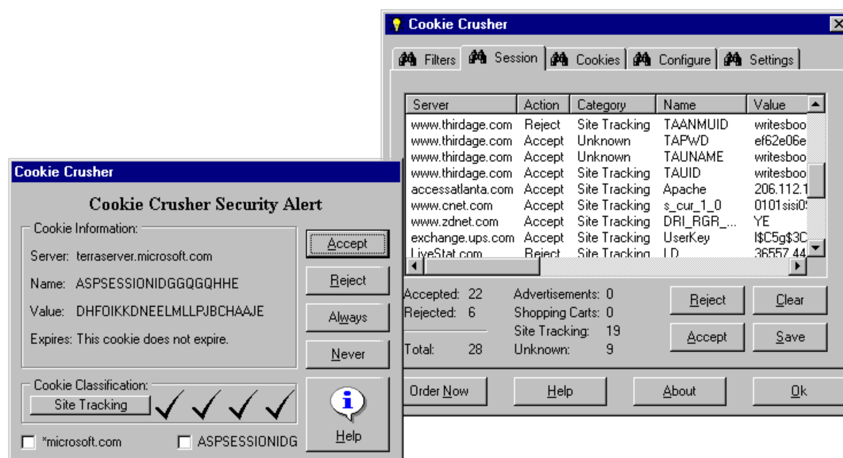
עלעל מטה בתיבת הדו-שיח לחלק של ה-Cookies. כאן יש לך אפשרות לחסום, להרשות הכל, או לקבל הודעה על Cookies הנשלחים אליך באופן אקראי, ו/או Cookies הנשלחים אליך רק בפעם הראשונה שאתה נכנס לאתר אינטרנט.

תוכנות לבקרה על Cookies

אפשרות אחרת לבקרה על Cookies היא להשתמש בתוכנה שנועדה למטרה זו. ישנן כמה כאלו, כולל תוכנות שיתופיות. להלן פירוט של שתיים מהן.

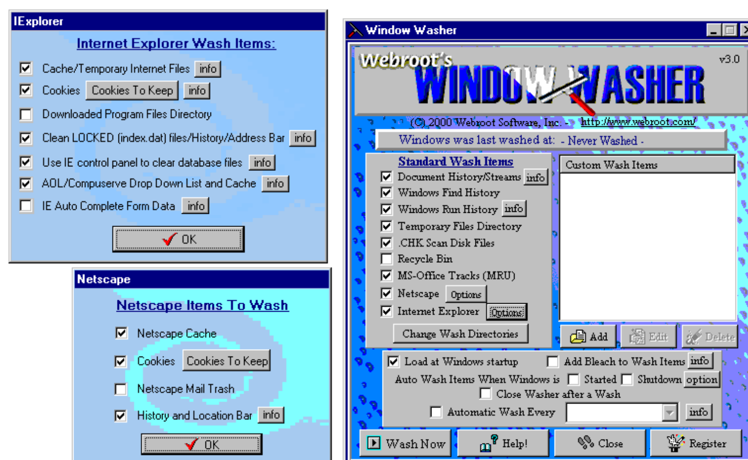
❖ Cookie Crusher (הכלולה בתקליטור המצורף לספר זה) היא תוכנה שיתופית החוסמת או מנהלת Cookies, כרצונך, בזמן אמת. היא מאפשרת גם לצפות בכל Cookie הנשלח למחשב ולהחליט אם להרשות לו להיכתב לקובץ. תרשים 11.4 מתאר את Cookie Crusher בפעולה.

❖ תוכנה שיתופית טובה נוספת היא Window Washer (הכלולה אף היא בתקליטור המצורף). Window Washer עושה ניקוי מלא של קבצים חסרי ערך, אך יכולה להתמקד רק בקבצי הזבל של Netscape או Internet explorer.



תרשים 11.4 Cookie Crusher, תוכנה לניהול Cookies

Window Washer גם מאפשרת הגדרת איזה Cookies ברצונך לשמור, כמתואר בתרשים 11.5 שלהלן.



תרשים 11.5 Window Washer מנקה סוגי קבצים רבים ומציעה אפשרויות יעילות לניקוי קבצי אינטרנט

יש עוד דרך אחת למנוע מ-Cookies להגיע למערכת שלך. כפי שנדון בסעיף הבא, **Proxy Server** יכול למנוע מ-Cookies להיכנס למערכת ולספק גם יתרונות נוספים.

גלוש אנונימית עם Proxy Server

האם רצית לבקר באתר אינטרנט אך חששת שמא האתר מתעד את ביקורך ואוסף מידע אודותיך? אולי לא רצית שייוודע מאיפה הגעת (למשל, בעת גלישה ממחשב במקום העבודה כדי לבקר אתר מתחרה). או, אולי אתה חוקר בעיה רפואית ואינך מעוניין שזה ייוודע - בוודאי לא לחברות ביטוח שיש להן גישה לאתרים שביקרת במחקריך.

ישנה גם אפשרות שמישהו עוקב אחריך אישית, או אולי ביקרת באתר מפוקפק, ואינך רוצה שאיש יידע על כך.

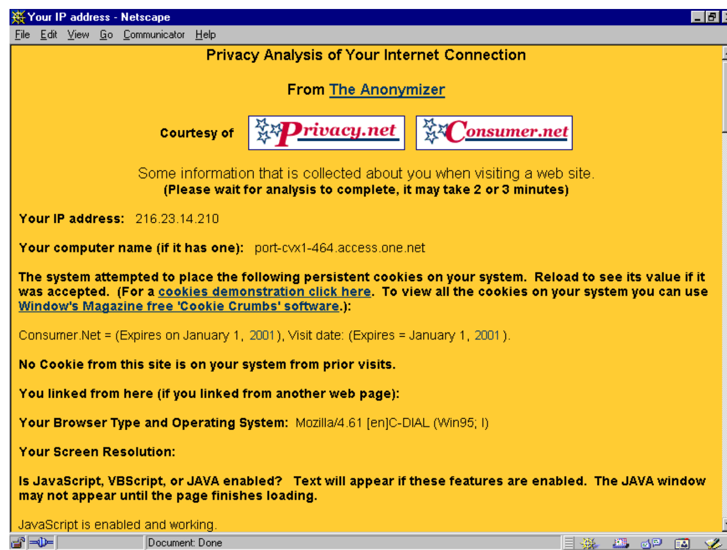
פרט לסיבות אלו, אולי פשוט אינך מעוניין לתרום לדמוגרפיה השיווקית של מישהו. אין זה משנה מהן סיבותיך לרצות בביקור אנונימי באתרי אינטרנט, שרת Proxy עשוי לסייע לך.

שרת Proxy הוא סוכן המגונן על זהותך באתר בו אתה מבקר. בגלישת אינטרנט רגילה, המערכת שלך מחליפה נתונים עם האתר המארח, ודפי האינטרנט שאתה מבקש משודרים אליך. על פניו, נראה שהמידע היחיד שאתה מוסר הוא כתובת URL הרצויה. לא נכון! המערכת המרוחקת עשויה לאסוף מידע רב נוסף מהמחשב שלך כולל - אך לא רק - שמך בספק האינטרנט, כתובת דואר אלקטרוני, וכתובות URL שביקרת בהן קודם.

כדי לקבל מושג מה ניתן ללמוד עליך בעת ביקור באתר אינטרנט, בקר בדף הבא: http://privacy.net/anonymizer/. תרשים 11.6 מראה מעט ממה שנתגלה כאשר ביקרתי באתר זה.

זהו רק חלק מהמידע המושג. כפי שראית, מידע רב אודות המחשב זמין בקלות באתר האינטרנט, כגון רשימה של כל תוספי התוכנה של הדפדפן (Browser Plug-Ins) המותקנים, ועוד, כולל פרטים על ספק האינטרנט, מי הבעלים של הרשת, דף האינטרנט בו ביקרת לפני שהגעת לאתר זה, האם תוכנה מסוימת פעילה, ואיזה סוגי קבצים הדפדפן שלך מוגדר לקבל.

אם תשתמש בשרת Proxy, אף פריט מידע מסוג זה לא יגיע לאתרים בהם תגלוש. כמו כן, Cookies לא נכתבים לדיסק הקשיח שלך מהאתרים בהם ביקרת.



תרשים 11.6 חלק מהמידע שאתר אינטרנט מקבל על כל גולש

כיצד עובד שרת Proxy?

שרת Proxy עומד בינך לבין האתר המארח באינטרנט. במקום שהדפדפן שלך יבקש דפים מהשרת, שרת Proxy עושה זאת עבורך, ואז מעביר את הדפים אליך. כל אתר בו אתה מבקר חושב שהמבקר הוא שרת ה-Proxy ולא אתה. שום מידע אישי שלך לא נאסף על ידי האתרים בהם ביקרת. לא ניתן אפילו לדעת מהיכן אתה בעולם.

שרתי אינטרנט של חברות רבות משתמשות בשרתי Proxy כדי לבודד את עצמם משאר הרשת. היחס בין שרת Proxy לשרת חברה בהקשר זה דומה ליחס של שרת Proxy לדפדפן שלך. שרת Proxy מאחזר דפים נדרשים מהאינטרנט, ומעבירים הלאה לשרת החברה בלי שיווצר קשר כלשהו עם מקור הדפים שאוחזרו. שרתי אינטרנט של חברות נוהגות לרוב לסנן או לחסום גישה לסוגים מסוימים של אתרי אינטרנט, כמובן. שרתי Proxy מיוחדים יידונו בסעיפים הבאים.

ה-Anonymizer: שרת Proxy פשוט

אחד משרתי ה- Proxy מבוססי האינטרנט הנפוצים יותר (והקלים ביותר לשימוש) הוא Anonymizer ‏(http://www.anonymizer.com), כמתואר בתרשים 11.7. ל-Anonymizer יש ממשק משתמש פשוט. עליך לגשת לשורת הכתובת בחלק העליון של החלון, להקיש את הכתובת אליה אתה רוצה לגשת (URL), ואתה בדרכך - האנונימית.



תרשים 11.7 Anonymizer, שרת Proxy פשוט

Anonymizer גם מספק רשימת קישורים גדולה אליהם תוכל לעבור בצורה אנונימית. בנוסף לכך שהוא מאפשר גלישה אנונימית באינטרנט, הוא גם יכול לשמש לגישה אנונימית לאתרי FTP.

כאשר אתה מקליד כתובת של דף אליו אתה רוצה לגשת באינטרנט, הוא יוצג בפניך כפי שהוא מתארח ב-Anonymizer. תרשים 11.8 מתאר כיצד זה נראה, כולל כרזת פרסום של-Anonymizer .

Anonymizer הוא שירות מסחרי אך ניתן להשתמש בו בחינם. אולם, תיאלץ להמתין כ- 30 שניות לטעינת כל דף, וכך תראה את הפרסומות.



תרשים 11.8 דף אינטרנט כפי שנראה באמצעות שרת Proxy של Anonymizer.

שרתי Proxy ציבוריים אחרים

שרתי Proxy אחרים מסחריים וחופשיים נמצאים באתרים להלן:

ByProxy: http://www.besiex.org/ByProxy/index.html

MagnusNet: http://www.magnusnet.com/proxy.html

Proxymate: http://lpwa.com:8000/

מחיקת עקבותיך המקוונים באמצעות תוכנה

בנוסף ל-Cookies, הסימניות (Bookmarks, Favorites) וקבצי האינטרנט הזמניים יכולים להסגירך אף הם. סעיף זה דן בהגנה על תחומים אלה.

הפסק להסגיר את עצמך עם סימניות

סימניות נקראות Bookmarks ב-Netscape, ו-Favorites ב-Internet Explorer.

אם גלשת באינטרנט מספר פעמים, ודאי צברת לא מעט סימניות. אלו נשמרות בקובץ סימניות bookmarks.htm ב-Netscape, וברשימת מועדפים (תיקיה C:\Windows\Favorites) על ידי Internet explorer.

ניתן להימנע מאיסוף סימניות או פשוט להעתיקם לקובץ - אשר, כמובן מגדיל את הסיכון שחטטן כלשהו יצפה בהם (ניתן גם פשוט לרשום אותן. אולם, שיטות אלו ימנעו ממך את הנוחות של לחיצה על URL ברשימה כדי להגיע לאתר מיידית).

סימניות פרטיות

ישנה חלופה. ניתן להשתמש בתוכנה חכמה בשם Private Bookmarks, הנמצאת בתקליטור המצורף. Private Bookmarks מצפינה את הסימניות או רשימת המועדפים שלך, כך שאיש מלבדך לא יוכל לראות את כתובות ה-URL של דפי האינטרנט ברשימה. תרשים 11.9 מתאר את ממשק המשתמש של התוכנה.



תרשים 11.9 תוכנת Private Bookmarks מסתירה או מארגנת את סימניות המועדפים

Private Bookmarks מבצעת מספר תפקידים שימושיים. תפקידה העיקרי הוא הצפנה והסתרת סימניות רשימות מועדפים. Private Bookmarks גם מייבאת ומייצאת רשימות, ומאפשרת ארגונן בקבוצות והדפסתן. הוספה והסרת URL היא פשוטה.

תוכנה שיתופית זו עובדת עם Netscape, Internet explorer, ורצה על כל גירסה של Windows.

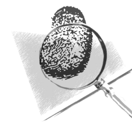
היפטר מקבצים המסגירים אותך

אחד הדברים הקשים יותר באבטחת המחשב הוא להיפטר מכל השאריות והזנבות שהאינטרנט משאיר במערכת לאחר כל התחברות. שאריות אלו כוללות דפי אינטרנט שלמים, גרפיקה, URL, קבצים זמניים, תוכנות Java ו-ActiveX, רסיסי דואר אלקטרוני נכנס ויוצא, Cookies, ועוד.

למדת הרבה על העקבות שגלישה ומשלוח דואר באינטרנט משאירים במערכת, בפרק 9. אך יש עוד - וחלקן אף קשה לאיתור.

למרבה המזל, קל להיפטר מכל אלו, בעזרת תוכנה מתאימה. יש תוכנות שתוכננו לנקות את שאריות האינטרנט, ורובן גם מנקות שאריות וזבל נוסף, כגון קבצים זמניים TMP. שנידונו בפרק 6.

שני מוצרים בקטגוריה זו הם Norton CleanSweep ו-Quarterdeck Remove-It שנבחנו כבר בפרק 6. תוכנה נוספת היא Window Washer, שנידונה קודם בפרק זה.



Window Washer מאפשרת הגדרת סוג הקבצים שיישארו לפני שהיא מתחילה לנקות את הדיסק. כמו כן התוכנה גם מאפשרת כתיבה חוזרת על אזור קובץ מחוק מספר פעמים כדי למנוע מתוכנת Unerase (שחזור מחיקה) מלשחזר קבצים שמחקת - תכונה שהיא חלק מ-Norton CleanSweep.

תוכנות מתמחות

אבטחה בזמן שהותך באינטרנט היא כמובן, חיונית. שתי תוכנות המסייעות בתחום זה הן McAfee Guard Dog, ו- Norton Internet Security 2000. שתיהן מגינות נגד וירוסים וסוסים טרויאניים העשויים להגיע עם Applets (יישומונים) של Java או בקרי ActiveX.

תוכנות אלו גם חוסמות או שולטות על Cookies בדפדפנים. Norton Internet Security 2000 הולכת אף צעד אחד הלאה בכך שהיא מגינה נגד איומים בצ׳טים של IRC וחוסמת פרסומות, ואף מספקת בקרת הורים להגבלת גישת ילדים לאינטרנט.

שתי התוכנות נידונות ביתר פירוט בפרק 8.

כמה מילים על תוכנות ניטור אינטרנט

בעת דיון על תוכנות ניטור וחסימת אינטרנט, מייד עולה המחשבה על הגנת ילדים מהתוכן שבכמה אתרים מפוקפקים הנמצאים באינטרנט, וניהול יומן על מעשיהם.

זה אינו היישום היחיד לתוכנות אלו. רבות מהן יכולות לתעד מה קורה במחשב במצב בלתי מקוון בנוסף למקוון. למעשה אלו תוכנות ״ציתות״ היכולות להעיד על כל מעשיך - אפילו על אמצעי האבטחה שנקטת! הן אף עלולות להראות מה הסיסמאות המקוונות והבלתי מקוונות בהן השתמשת.

כל זאת ניתן לעשות עם או ללא ידיעתך. תוכנה אחת מסוג זה - שגירסה ממנה משווקת לעסקים ממוחשבים, היא Cyber Patrol - הנמצאת באתר (http://www.microsys.com/business/). בנוסף ליכולתה לעקוב ולתעד פעילות

אינטרנט, היא גם מסוגלות לעקוב אחר פעילות לא מקוונת. תוכנה אחרת היא 007 Stealth Activity Monitor (SAM), המתוכננת לתעד ולשמור כל דבר במחשב (נמצאת בתקליטור המצורף), נדון בה בפרק 12. עליך לדעת שתוכנות כאלו עלולות להיות מותקנות ללא ידיעתך.

הכיצד? המחשב במקום עבודתך ניתן לגישה על ידי אחרים, כמובן, ואין כל דרך למנוע התקנת תוכנה בו. באשר למחשב בביתך, מישהו יכול לעקוף את הגנת הסיסמה על ידי שימוש בדיסקט עם מערכת הפעלה DOS כדי לאתחל אותו (זה כולל עקיפת סיסמאות אתחול, כפי שנידון בפרק 3).



כדי למנוע עקיפה של סיסמת אתחול המערכת, עליך לבטל אפשרות אתחול מדיסקט (לרוב כונן A). תחילה, גש להגדרות המחשב (CMOS), על ידי לחיצה על F1 או Delete או מקש דומה בעת אתחול המערכת (בעת האתחול תופיע הודעה המורה איזה מקש ללחוץ). בתפריט המתקבל, חפש הגדרה מסוג "Boot Options" או דומה.
עקוב אחר ההנחייה עד שתמצא הגדרה Enable/Disable, ל- Boot From Floppy, Check Drive A (אפשר/בטל אתחול מדיסקט, בדוק כונן A), או בדומה לכך.

אינטרנט למבוגרים בלבד?

יש הרבה מיסתורין סביב האינטרנט. קריאת עיתונים ושמיעת ידיעות ברדיו ובטלוויזיה על דברים המתרחשים באינטרנט, עשוייה לצייר תמונה מוטעית למי שעדיין לא התחברו (מרבית האוכלוסייה) לאינטרנט. חלק מהאנשים שמע עד כמה האינטרנט ממכרת - ממש כמו סמים, חלקם מניח שהאינטרנט היא רשת תקשורת שהוקמה על ידי חבורת נוכלים בינלאומית לצורך העברת מספרי כרטיסי אשראי גנובים ומנגד, חלקים נרחבים בציבור תופסים את האינטרנט ככלי המשרת דווקא חבורת סוטים, מציצנים ואחרים שעיסוקם במין, המנסים לתפוס ברשתם את המשוטטים ב-CyberSpace. המונחים הקשורים לאינטרנט תורמים גם הם למיסתורין, במיוחד אם הם נאמרים באנגלית: CyberSpace ו-CyberSex, Information SuperHighWay, Web, GopherSpace, Virtual Mall ועוד צירופים רבים אחרים הכוללים את המילים Cyber ו-Space.

המונח CyberSpace מתייחס לרשת בינלאומית של רשתות מחשבים. זוהי ה"אמא" של כל הרשתות. כל אחד יכול להתחבר אליה ללא הבדל מיקום גאוגרפי, דת, גיל או צבע עור, וכל זאת - במחיר נמוך. מרבית המידע הנמצא במחשבים המרכיבים את הרשת (ומספרם נמדד במיליונים) הינו מידע שימושי ומועיל. להלן רשימה חלקית ביותר של סוגי המידע באינטרנט: ידיעות שונות, מידע ממשלתי, מאמרים מהעיתונות, מידע מסחרי על חברות וגופים עסקיים, מידע אוניברסיטאי לנרשמים וכן, יש גם סקס.

מדי פעם עולה הוויכוח סביב היכולת לצנזר את המידע המועבר באינטרנט. בתי המשפט בארה"ב רואים בצנזורה על האינטרנט פגיעה בחופש הפרט ובחופש הביטוי הנוגד את החוקה. זהו עוד שלב במאבק על האינטרנט, שנמשך ועתיד להימשך עוד. בית המשפט רואה את ההתחברות לאינטרנט והעבודה באינטרנט כשיחת טלפון מתמשכת. לכן פסיקתו היתה שמכיון וזוהי שיחה פרטית יהיה זה מעשה בלתי חוקי לצותת ולצנזר אותה.

פרשת מוניקה או בשמה 'מוניקהסקס' העלתה מחדש את הוויכוח. מאות דפים מהדוח של החוקר המיוחד קנת סטאר, מתארים בפרטי פרטים את מעשיהם של קלינטון ולוינסקי בחדרי הבית הלבן. זה לא עוד תיאור של גיבור מאיזה שהוא רומן המקיים יחסים עם אישה מסתורית, זהו נשיא ארה"ב!

הדוח של קנת סטאר יורד לפרטי פרטים ומתאר מפגש אחר מפגש את הרומן עם הגברת לוינסקי. כל אחד יכול לקרוא את הדוח באינטרנט, שם הוא פורסם במלואו לראשונה. באתר CNN בלבד, נרשמו 300,000 כניסות לדקה (אני חוזר, 300,000 כניסות לדקה). האתרים בהם פורסם הדוח מיהרו להזהיר את הגולשים מפני "מידע בלתי הולם".

מה יכול להסיק ילד שקורא את הדוח של סטאר:

- אם נשיא ארה"ב משקר אז גם אני יכול?
- על קיום יחסי מין מחוץ למסגרת הנישואין צריך רק לבקש סליחה?

הוויכוח סביב הסקס באינטרנט הוא **לא** אם יש הרבה או מעט סקס באינטרנט, וגם **לא** אם הסקס באינטרנט הוא "רך" או "קשה", אלא האם הסקס באינטרנט מיועד למבוגרים בלבד? אם התשובה היא כן, אז מייד עולה השאלה "איך נמנע מאלה שאינם מבוגרים גישה לאותו מידע?" בשלב זה הרחקנו לכת מעבר לעניין הסקס, כי אם היום נחליט לחסום את הגישה לאוכלוסייה מסוימת למידע המקוטלג תחת הערך "סקס", אז מי ימנע את האפשרות שמחר יחסמו לנו את הגישה למידע המקוטלג תחת הערך "אמנות"? לא אכנס במאמר זה לדיון פילוסופי נרחב, ורק אציין שיש לדיון שכזה משמעויות חוקתיות, חברתיות, פוליטיות ואחרות, ובוודאי יימצאו אנשי אקדמיה שיערכו מחקרים בנושא. ובאופן מעשי, ילדים יכולים להגיע לאתרים בהם מוצג מידע בנושאי מין, כגון תמונות, סרטי וידאו, או מאמרים. האפשרות שגם ילדים יקחו חלק בדיונים שונים שנושאם הוא מין גורמת להורים לסרב "להכניס" את האינטרנט הביתה.

העניין סביב הכנסת, או אי-הכנסת האינטרנט הביתה בגלל החשש לשימוש לא נאות בידי הילדים, דומה לחששות שהתלוו לכניסת מכשיר הווידאו הביתה וההתחברות לכבלים. למכשיר הווידאו ניתן להכניס קלטת ובה מידע מכל סוג שהוא: סרט לכל המשפחה, קלטת הדרכה לבישול, קלטת פעילות לילדים, וגם סרטים כחולים (הקרויים XXX). כדי למנוע מילדים להכניס את הקלטות האסורות, הומצאו כל מיני מנעולים הניתנים לתכנות במכשיר הטלוויזיה, וגם מנעולים מכניים. אחר כך הגיעו הכבלים עם הסרטים האסורים בערוץ הגרמני, שעכשיו מוקרנים גם בערוצים המקומיים עם תרגום, ועדיין לא הומצא פטנט לחסימתם. ומהן שיטות החסימה באינטרנט?

תעשיית התוכנה התגייסה לנושא ופיתחה מספר תוכנות, כמו: CyberSitter (על משקל BabySitter), Net Patrol, SurfWatch, Net Nanny, SafeSurf ועוד. התוכנות אמורות לחסום את הגישה לאתרים במספר שיטות מגוונות ומעניינות. הורה שרוצה להפעיל בקרה ולקבוע כללי גישה לילדיו יקבל לידיו כלי, שהוא הרבה יותר יעיל מחוסר אמצעים כלל. הבשורה הטובה היא שאכן תהיה חסימה, והבשורה הרעה היא שבשיטת החסימה בעזרת התוכנה יש להורה הרבה עבודה, שאחריה עדיין יש פרצות גדולות מאוד.

כיצד זה עובד?

התוכנות משתמשות בדרך כלל ביותר ממנגנון אחד לצורך החסימה:

סינון - התוכנה מסננת כל פיסת מידע המגיעה למחשב מהאינטרנט, ומוחקת את המילים שהוגדרו כמילים "אסורות" כמו Sex, breasts ועוד הרבה אחרות (כולן באנגלית). התוכנה מגיעה, בדרך כלל, עם רשימה מכובדת של מילים "אסורות".

חסרונות:

- צריך לתחזק את הרשימה: להוסיף, למחוק ולעדכן.

חסמים - תוכנות מסוימות מאפשרות להורה לקבוע רשימה של אתרים "אסורים" לגישה, ו/או שמות של קבצים "אסורים" להורדה או צפייה. התוכנה מגיעה, בדרך כלל, עם רשימה מכובדת של אתרים "אסורים".

חסרונות:

- דורש מעקב ועדכון של אתרים חדשים ברשת וכאלה יש לפחות 50,000! כל יום. מספר זה הולך וגדל, שלא לדבר על זמן העיון הדרוש בכל אתר כדי לקבוע את "כשירותו".
- העדכון קשה מאוד, מכיון שהכתובות באינטרנט משתנות בקצב מסחרר.
- התוכנה תחסום קובץ בשם Sex02.gif, למשל, אבל לא קובץ בשם anderson.gif (פמלה אנדרסון ממשמר המפרץ בתמונת עירום).

עוקבים - אם אי אפשר לחסום, הבה נעקוב. זוהי קופסה שחורה הרושמת את כל האתרים שאליהם ניגשת ואת הקבצים שהורדת. בשיטה זו ההורה יכול לדעת היכן "שוטטו" ילדיו באינטרנט.

חסרונות:

- מחייב את ההורה להציץ מדי פעם ברשימה.
- הורה שיראה שילדיו היו באתר /http://www.free-sex.com לא יכול לקבוע אם זהו אתר "מותר", או אתר "אסור"?

סיסמה - זהו מנגנון נלווה למנגנונים שצוינו לעיל. לדוגמה: כאשר נעשה ניסיון לגשת לאתר "אסור", החסם מופעל ומופיעה האפשרות להכנסת סיסמה. סיסמה נכונה תאפשר כניסה לאתר והצגת המידע.

חלק מהאתרים, לדוגמה, משתמשים בדירוג שנקרא RSAC. הדירוג ניתן לפי רמת האלימות, ניבול הפה, סקס ועירום. בתור הורה תוכל לקבוע את הדירוג המתאים לכל אחד מבני המשפחה. מי שינסה להיכנס לאתר שאין לו הרשאה מתאימה, יתבקש לבקש רשות מההורים ולהקליד סיסמה.

חסרונות:

- מישהו מגדיר עבורך מהי "נשיקה בתשוקה", "נגיעה מינית בבגדים", "נגיעה מינית מרומזת", "פעילות מינית ברורה".
- הידעת שאתר פלייבוי מוגדר בדירוג RSAC בתור "נגיעה מינית מרומזת".
- רוב האתרים אינם מדורגים ולכן לא תוכל להיכנס אליהם.

לכל המנגנונים שצוינו לעיל יש מספר חסרונות גדולים:

- אף אחד, גם ילד בן 12, לא אוהב שמישהו ישים עליו צנזורה.
- אפשר לא להפעיל את תוכנת החסימה והסינון, ואז הכל פתוח.
- אפשר "לשבור" את התוכנה, לפצח את הסיסמה ו"לפברק" לאבא ואמא רשימת אתרים - זה קל, וכל "ילד בן 12" מסוגל לעשות זאת!

אז מה עושים?

הנה רשימה של מספר כללים פשוטים שיכולים לעזור. כללים אלה ניתנים להפעלה ללא קשר אם מופעלת תוכנת צנזורה/בקרה כזו או אחרת. כל אחד מהם וגם שילובם יחדיו, לא ימנעו באפקטיביות של 100% את הגישה של ילדיכם לאתרי סקס. אם הם ירצו - הם יגיעו לשם ודבר לא ימנע בעדם לעשות זאת.

הפוך את השימוש באינטרנט לבילוי לכל המשפחה:

- הצב את המחשב המחובר לאינטרנט בחדר המשפחה עם המסך לכיוון פנים הבית.
- הצץ במסך מדי פעם.
- דבר עם ילדיך באופן חופשי על האינטרנט, כמו שאתה מדבר איתם על כדורגל, חברים או אוכל.
- הצטרף מדי פעם לגלישה עם ילדיך באינטרנט.

תן הנחיות ברורות לילד אודות השימוש באינטרנט:

- אף פעם לא למסור שם מלא, כתובת מגורים, כתובת בית הספר ומספרי טלפון ללא רשות ההורים.
- יש לילד זכות מלאה לעזוב אתר בו מוצג מידע הגורם לו אי-נוחות.
- יש לילד זכות מלאה לצאת מדיון אם הנושא לא נראה לו או מעורר בו שאט-נפש.
- אסור לילד להסכים לפגישה עם מישהו שהכיר דרך האינטרנט.

בקרה

- בדוק את חשבון ההתחברות לאינטרנט כדי לוודא שהתקשורת לאינטרנט נעשתה בשעות סבירות ובהיקף מתאים, ולא על חשבון פעילויות אחרות.
- מדי תקופה בדוק את חשבון הטלפון של בזק, כדי לאתר מספרי התקשרות לתחנות BBS ולא רק לאינטרנט.

מניעת הגישה ל-CyberPorn דומה ל"מלחמה" שאתה, כהורה, עורך כנגד סמים ואלכוהול. זוהי "מלחמה" מתמשכת שבה אתה מגייס את כל הכלים שעומדים לרשותך. ב"מלחמה" הזאת אתה לא לבד, גם הממשלה והרשויות לוחמות לצידך. אל תחכה להם - היה פעיל. אל תחכה שאחרים יעשו את המלחמה הזאת בשבילך. הסבר לילדיך מה מותר ומה אסור - כדי שיבינו. היה ערני לאופן השימוש שלהם באינטרנט, והזכר לעצמך מדי פעם כי אחרי שילדך יראה את נערת החודש של פלייבוי על מסך המחשב, הוא יראה את הפאואר ריינגרס, WWF, צילומי חדשות מאזורי הקרבות בבוסניה ועוד, על מסך הטלוויזיה.

כיצד אדע אם מצותתים לי?

לא משנה מהן נסיבות ההתקנה, בכל מצב ניתן להסתיר תוכנות ניטור אינטרנט. כולן תוכננו לעבוד ברקע, בצורה בלתי מורגשת על ידי המשתמש.

יתכן שתוכל לגלות תוכנה של חטטן כלשהו, מתוך תפריט **התחלה (Start)**, לחץ על **תוכניות (Programs)**. ושוב, אולי לא. חלק מתוכנות הניטור מתוכננות לא להיראות בתפריט התוכנות, והן אינן יוצרות קיצורי דרך על שולחן העבודה בעת התקנתן.

היעדר ראיות ממשיות לקיום תוכנת ניטור במחשב, משמעו שעליך לחפשה (שים לב שההתייחסות כאן היא בעיקר למחשב לא מרושת. אם אתה משתמש במחשב ברשת, יש סיכויים קלושים בלבד שתוכנת חטטן תונח בדיסק המקומי).

חיפוש תוכנה מוסתרת כרוכה בעיקרה בהפיכת הכיוון של מה שלמדת לעשות בעת הסתרת תוכנות ותיקיות. המקום הראשון לחפש בו הוא רשימת המסמכים של תפריט **התחלה (Start)**, ולחיצה על **מסמכים (Documents)**. אולי תגלה שחטטן עיין בקובץ יומן המתעד את מעשיך.

הפעל את **סייר Windows** - ודא שצפייה בקבצים נסתרים מאופשרת. עתה הסתכל בתיקיות הבאות וחפש קבצי תוכנה או תיקיות חדשות:

- תיקיית השורש של הדיסק הקשיח (לרוב \:C או \:D).
- קבצי תוכנה
- Windows
- Windows/System

כמו כן חפש בסל המיחזור לראיות על חטטנות, כגון קבצי יומן מחוקים.

אם יש לך תוכנת ארכיב כגון Aladdin Expander, PKZIP, או WinZip, הפעל אותה ועיין בתפריט **קובץ** שלה. ייתכן שתגלה שחטטן נאלץ לפרוש (Unzip) קבצי תוכנה כדי להתקינה, ואף שמחק את קובץ ZIP המקורי, הוא השאיר עקבות בתפריט הקבצים של תוכנת הארכיב.

התקנת תוכנה גם עשויה להשאיר עקבות בקובץ האצווה של המערכת Autoexec.Bat ובקובץ Config.sys. אינך חייב לבחון את תוכן הקובץ, שרובו ככולו יהיה חסר משמעות. במקום זאת, בדוק את מאפייניהם עם סייר Windows. גש לתיקיה הראשית של כונן C; לחץ לחיצה ימנית על הקובץ האמור. אם התאריך חדש מאוד, ייתכן שמישהו שינה את ההגדרות באמצעות התקנת תוכנה. כמו כן יש לבדוק את הקובץ Win.Ini, הנמצא בתיקיה Windows\.

אם אכן תגלה שאתה מצותת, נסה להסיר את תוכנת הניטור. אם מתברר שנדרשת לכך סיסמה, פשוט מחק חלק מקבצי התוכנה באמצעות סייר Windows. זה יגרום לתוכנה להיות בלתי ניתנת להפעלה. ודא שאתה מתעסק עם קבצי התוכנה הנכונים, כמובן! זה פשוט ביותר אם לתוכנה יש תיקיה משלה.

המקרה של הבעל החטטן

לא מזמן נודע לי מקרה על אישה שהיתה גרושה מספר חודשים, אך בעלה לשעבר המשיך לעקוב אחר מעשיה מקרוב. עד כמה קרוב, לא היה לה כל מושג, עד שהוא צלצל אליה יום אחד וסיפר לה בפרטי פרטים על השיחה הרומנטית שניהלה בצ'ט מקוון - ומי הם האנשים ששלחו לה תמונות של עצמם בדואר אלקטרוני.

התוכנה שהתקין, במחשב של אשתו לשעבר, היתה מאתרת קבצים מסוימים ושולחת אותם באמצעות דואר אלקטרוני היישר אליו.

כפי שהתברר, הוא התקין את התוכנה לפני הגירושים והפעיל אותה בעת ביקור. היה ניתן למצוא את התוכנה - אף שהיא מחקה את עצמה לאחר שליחת מספר קבצים בדואר אלקטרוני.

יש כאן שני לקחים: הראשון, עליך באמת לשים לב מי מתעסק עם המחשב שלך. הלקח השני הוא שלעיתים לא בטוח לאחסן במחשב מידע העשוי להעמידך במצב לא בטוח.

אני מקווה שעכשיו אתה מוכן לשמור את קבציך ופעולותיך הרגישים בטוחים, גם כשהם מקוונים וגם כשהם לא מקוונים. ובכל זאת, לא יזיק להתוודע לכמה כלים זמינים של חטטן מקצועי. אם אתה חש שפרטיותך בסכנה בבית או בעבודה, עליך לקבל מושג על הנשק העומד לרשות הצד השני במלחמה על הפרטיות - זאת נעשה בפרק 12.

גלוש אנונימית עם Proxy Server

האם רצית לבקר באתר אינטרנט אך חששת שמא האתר מתעד את ביקורך ואוסף מידע אודותיך? אולי לא רצית שייוודע מאיפה הגעת (למשל, בעת גלישה ממחשב במקום העבודה כדי לבקר אתר מתחרה). או, אולי אתה חוקר בעיה רפואית ואינך מעוניין שזה ייוודע - בוודאי לא לחברות ביטוח שיש להן גישה לאתרים שביקרת במחקריך.

ישנה גם אפשרות שמישהו עוקב אחריך אישית, או אולי ביקרת באתר מפוקפק, ואינך רוצה שאיש יידע על כך.

פרט לסיבות אלו, אולי פשוט אינך מעוניין לתרום לדמוגרפיה השיווקית של מישהו. אין זה משנה מהן סיבותיך לרצות בביקור אנונימי באתרי אינטרנט, שרת Proxy עשוי לסייע לך.

שרת Proxy הוא סוכן המגונן על זהותך באתר בו אתה מבקר. בגלישת אינטרנט רגילה, המערכת שלך מחליפה נתונים עם האתר המארח, ודפי האינטרנט שאתה מבקש משודרים אליך. על פניו, נראה שהמידע היחיד שאתה מוסר הוא כתובת URL הרצויה. לא נכון! המערכת המרוחקת עשויה לאסוף מידע רב נוסף מהמחשב שלך כולל - אך לא רק - שמך בספק האינטרנט, כתובת דואר אלקטרוני, וכתובות URL שביקרת בהן קודם.

כדי לקבל מושג מה ניתן ללמוד עליך בעת ביקור באתר אינטרנט, בקר בדף הבא: http://privacy.net/anonymizer/. תרשים 11.6 מראה מעט ממה שנתגלה כאשר ביקרתי באתר זה.

זהו רק חלק מהמידע המושג. כפי שראית, מידע רב אודות המחשב זמין בקלות באתר האינטרנט, כגון רשימה של כל תוספי התוכנה של הדפדפן (Browser Plug-Ins) המותקנים, ועוד, כולל פרטים על ספק האינטרנט, מי הבעלים של הרשת, דף האינטרנט בו ביקרת לפני שהגעת לאתר זה, האם תוכנה מסוימת פעילה, ואיזה סוגי קבצים הדפדפן שלך מוגדר לקבל.

אם תשתמש בשרת Proxy, אף פריט מידע מסוג זה לא יגיע לאתרים בהם תגלוש. כמו כן, Cookies לא נכתבים לדיסק הקשיח שלך מהאתרים בהם ביקרת.

פרק 12



מבט מהצד השני

מה בפרק:

- מפצחי סיסמאות
- פתרון לחוסר האבטחה של דואר אלקטרוני
- תוכנות יומן חמקניות
- ריגול היי-טק עם מערכת TEMPEST
- האקרים ודברים אחרים שמחוץ לשליטתך

בפרק זה נתמקד בצד השני של אבטחת המחשב: התחבולות וכלי התוכנה העשויים לשמש לחדירה לפרטיותך. כמו כן נבחן כמה מכלי התוכנה העלולים לשמש למטרות נפשעות, ונראה כיצד תוכל להגן על עצמך מפלישה מפניהם.

סיסמאות הן יסודות אבטחת המחשב. הפרק פותח לכן, במידע שמיש על פיצוח סיסמאות וכיצד למנוע זאת. מכאן, נעבור להתחברות ולתוכנות חמקניות אחרות (שסכנותיהן פורטו בפרק 11). אבטחה ואי-אבטחת דואר אלקטרוני יהיו הבאים בתור, עם דגש על שירותי דואר אלקטרוני מבוססי-אינטרנט.

משם נעבור לעולם המורכב של מעקב באמצעות Tempest ופריצה למחשב.

אבטחה ואי-אבטחה באמצעות סיסמאות

הגנה באמצעות סיסמה היא הכרחית. אנו משתמשים בסיסמאות במחשב, להתחברות לספקי שירות אינטרנט או שירותים מקוונים, להתחברות למחשב כמשתמש, וכן הלאה.

מכיון שסיסמאות כה חיוניות, לא מפתיע שפותחו תוכנות המיועדות לפצח אותן. בהתאם למטרותיך, תוכנה מסוג זה יכולה לשמש לאבטחה או לבילוש.

מובן שחטטן משתוקק לדעת מהן סיסמאותיך. זה יהפוך את המעקב אחריך פשוט וקל. באותה מידה, כמובן שאינך משתוקק שהסיסמאות יתגלו - אך הן עשויות להתגלות בנסיבות מסוימות או בעזרת כלים מסוימים.

השורה התחתונה היא: כי כל אחד יכול להשיג את הסיסמה שלך. כל שנדרש הוא גישה למחשב ו/או חשבונותיך המקוונים, התמדה, סבלנות, זמן וידע בכלים המתאימים.

מתוך ידיעת אפשרות זו, חשוב לשמור על סיסמתך. הקפד לא לרשום אותה בשום מקום, לא לשתף בה איש, והקשה על כל אחד, ככל הניתן, לנחש את סיסמתך.

עתה, נבחן כיצד מישהו שרוצה את סיסמתך ינסה לגלות אותה.

פריצה למחשבים באמצעות גילוי סיסמאות (Hacking)

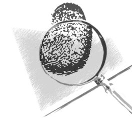
הזכרנו זאת בעבר, אך רצוי לחזור על כך: אל תיצור סיסמאות המבוססות על דבר מה בעל אופי אישי. סיסמאות המבוססות על שמות, תאריכי לידה, או מידע אישי אחר על קרוביך, חברים קרובים, חיות מחמד, ילדים, וכו', קלות מדי לניחוש על ידי כל אדם שיודע עליך אפילו רק מעט.

כמו כן, סיסמאות המבוססות על תחומי העניין האישיים שלך, או שמות קבוצות ספורט או סופרים או שחקנים, ניתנים לניחוש. הן אולי קלות לזכירה, אך הן קלות באותה מידה לניחוש.

במקרים רבים, להפתעתם וחרדתם, הראיתי לחברים כמה קל לנחש את סיסמתם. יש לך כלבה בשם Sophie? מה בדבר הסיסמה Sophie1 או Sophierun, או Sophiedog? יום ההולדת של ילדיך הוא 17 במרץ 1997? אולי הסיסמה היא 970317?

הרעיון ברור. עם מעט ידע מוקדם, כל אדם יכול לנחש מספר אפשרויות סיסמה. אחת מהן (או גירסה שלה) סביר שתהיה הסיסמה הנכונה. לכן, הסיסמה שלך לא צריכה להתייחס לדבר מה הקשור אליך.

סיסמה כזו אולי קשה לזכור. אולם, תגלה שאחרי שתשתמש בה שלוש-ארבע פעמים, הסיסמה תישאר חרוטה בזיכרונך. כמו כן רצוי להחליף את הסיסמה על בסיס קבוע - לפחות כל ארבעה עד שישה שבועות. כך, אם מישהו ישיג את סיסמתך היא לא תשמש אותו לאורך זמן.



כדאי לוודא שהסיסמה שהוקצתה לך על ידי ספק שירות אינטרנט, או אתר אינטרנט אינה מבוססת על שמך או התאריך בו נרשמת, שכן הן קלות לגילוי על ידי מישהו אחר המשתמש באותו השירות.



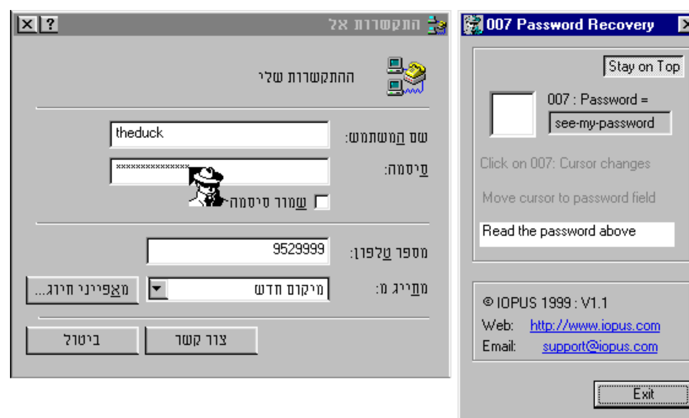
ככל שהסיסמה ארוכה יותר, כן ייטב. קשה יותר לנחש סיסמאות ארוכות. סיסמה המורכבת מאותיות וספרות רצויה. בנוסף, אם המערכת שלך מבחינה בין אותיות גדולות וקטנות, רצוי אף יותר להשתמש בה.

פריצה לסיסמאות באמצעות תוכנה

מתכנתים מפתחים תוכנות פיצוח סיסמאות זה זמן רב - ולא תמיד כדי לפרוץ למערכת של מישהו. יש מצבים בהם משתמש שוכח את סיסמתו ורוצה לפרוץ את סיסמתו שלו.

לדוגמה Windows מאפשרת אחסון והפעלה אוטומטית של סיסמאות שבשימוש רב, כמו הסיסמה לספק האינטרנט או דואר של Outlook Express. אם תאחסן את סיסמותיך, אתה עלול לשכוח אותן לאחר זמן מה. מה יקרה כשתצטרך את הסיסמה לשימוש במחשב אחר או תוכנה אחרת?

יש תוכנות שיראו לך מה הסיסמה מאחורי שורת הכוכביות (הכוכביות המופיעות במקום תווים בעת הקלדת הסיסמה). תוכנה אחת כזו היא 007 Password Recovery המתוארת בתרשים 12.1.



תרשים 12.1 007 Password Recovery תראה לך מה מסתתר מאחורי שורת הכוכביות בשדה הסיסמה של Windows



תוכנה זו, הנמצאת בתקליטור המצורף לספר זה, מציגה את הסיסמה שמאחורי הכוכביות. הפעל את התוכנה; לחץ והחזק את דמות המרגל , וגרור את הסמן ששינה צורתו לשדה הסיסמה.

007 Password Recovery פועלת היטב עם רוב מסכי הסיסמאות שתפגוש ב-Windows, כולל מסכי סיסמאות של אתרי אינטרנט. אך היא לא תעבוד עם יישומים המסתירים את הסיסמה "מאחורי" הכוכביות, כגון Windows NT User Manager.

ישנן תוכנות פריצת סיסמאות אחרות חזקות יותר שבהן ניתן להשתמש לפרוץ סיסמאות במחשב, יישומים, קבצים, וסיסמאות מקוונות. ההגנה הטובה ביותר כנגד אלו היא לא לאפשר לאחרים להשתמש במחשב שלך; כך, איש לא יכול להתקין ולהשתמש בתוכנות כאלו.

פתרון לחוסר האבטחה של הדואר האלקטרוני

כפי שצוין בפרק 10, דואר אלקטרוני עשוי להשאיר עקבות על המערכת שלך. אם אתה באמת מודאג מפרטיות דואר אלקטרוני, רצוי לנהל את פעילות הדואר האלקטרוני שלך מחוץ למערכת לחלוטין. זאת ניתן לעשות על ידי הצטרפות לשירות דואר אלקטרוני מבוסס אינטרנט.

שירותי דואר אלקטרוני מבוססי-אינטרנט, שנידונו בפרק 10, מספקים גישת דואר אלקטרוני מכל מחשב. כל שנדרש לקבלת דואר אלקטרוני הוא גישה לאינטרנט.

כדאי לציין ששירותים מקוונים אמינים ביותר, בעוד ששירותי דואר אלקטרוני מבוססי-אינטרנט עלולים להיתקל בעומס יתר או תקופות של ניתוק. עדיין, שירותי דואר אלקטרוני מבוססי אינטרנט הם **חינם**. וחלקם אף מספקים שירותי אינטרנט חינם.

תוכל לשמור את הדואר האלקטרוני שלך מקוון ולהימנע מהסיכון של השארת עקבות דואר אלקטרוני במחשב. אולם, תיאלץ לנקות את המערכת מעת לעת. לצורך כך, רצוי ביותר להשתמש באחת מתוכנות הניקוי הנידונות בפרק 11, אף שניתן לעשות חלק גדול מתחזוקת הניקיון בעצמך, כמוסבר בפרק 9. אם אתה משתמש בשירות דואר אלקטרוני מבוסס אינטרנט, אל לך להוריד קבצים מוצמדים לדואר אלקטרוני, ולא לכתוב הודעות חדשות או לענות במצב לא מקוון.

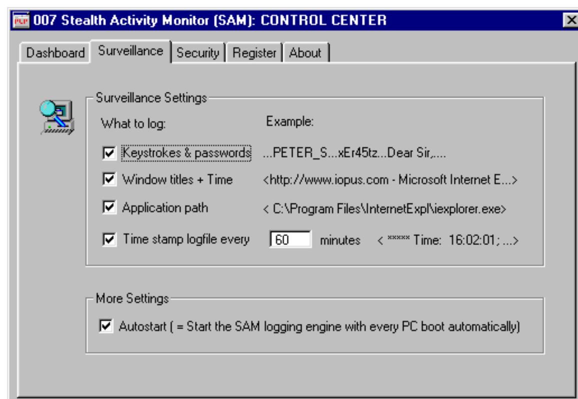
תוכנות יומן חמקניות

כפי שראית בפרק 11, ניתן לצותת למחשב שלך בלא ידיעתך, באמצעות תוכנה חמקנית. תוכנה מסוג זה מתעדת ושומרת מידע על אופן השימוש במחשב לצורך גישה מאוחרת יותר. מידע מתועד ונשמר יכול לכלול:

- את התאריך והשעה שבה משתמש התחבר או התנתק ממחשב (אם קיימת אפשרות לריבוי משתמשים).
- מתי תוכנות הופעלו או נסגרו.
- מתי בוצעה גישה לקבצים.
- מתי קבצים שונו ונשמרו.
- כתובות URL בהן ביקרת באינטרנט.
- קבצים שהורדו.
- קבצים שנמחקו.
- סיסמאות שהוקלדו, למחשב ובאינטרנט.
- כל מקש פקודה שהקשת.

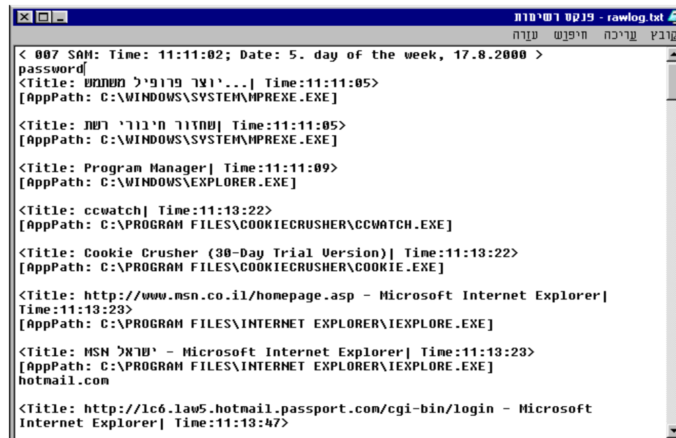
המידע עשוי להישמר במערכת שלך בתיקיה או בקובץ נסתרים, או להישלח בדואר אלקטרוני ללא ידיעתך.

תוכנה אחת מסוג זה היא 007 Stealth Activity Monitor (SAM). SAM תוכננה לבצע ניטור על כל מעשיך במחשב. כמתואר בתרשים 12.2, SAM יוצרת יומן הקשות מקלדת, נתיבי (תיקיות) תוכנות, ועוד. היא אפילו יכולה להראות מתי ניגשו לתוכנות מוסתרות.



תרשים 12.2 כמה הגדרות של תוכנת 007 Stealth Activity Monitor (SAM)

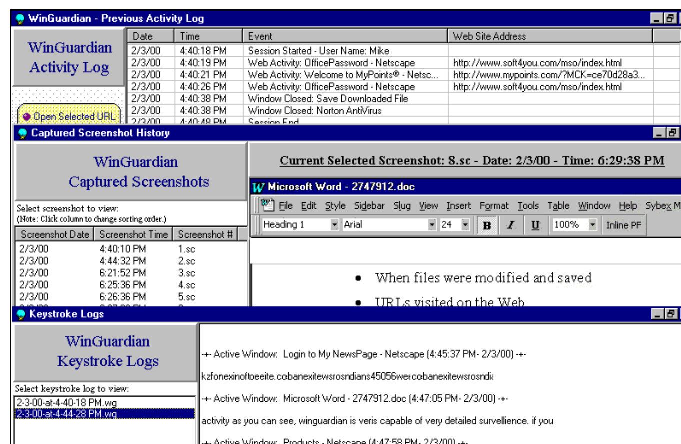
תרשים 12.3 מתאר דוגמת קובץ יומן של SAM. כפי שניתן לראות, הקובץ מפרט אילו תוכנות הורצו ומתי, אתרי אינטרנט שבהם ביקרת, סיסמאות מקוונות ולא מקוונות, ומעברים בין חלונות יישומים.



תרשים 12.3 קובץ יומן של SAM

ל-SAM יש קרוב מתקדם יותר, גם הוא כלול בתקליטור המצורף לספר זה, ששולח בסודיות דוחות באמצעות דואר אלקטרוני לכתובת מוגדרת. תוכנה זו, בשם STARR (Stealth Activity Recorder And Reporter), אוספת מידע מפורט יותר על המשתמש.

תוכנה נוספת מסוג זה היא WinGaurdian. היא מוצעת כתוכנה לניטור משתמשים, והיא מקיפה ביכולות המעקב שלה. ניתן לראות יומן פעילויות, הקשות, ואפילו תצוגות מסכים, כמתואר בתרשים 12.4.



תרשים 12.4 דוחות פעילות של WinGaurdian

WinGaurdian גם מסוגלת לערוך דוחות נפרדים על מיגוון סוגי פעילויות.

מה לעשות אם מצותתים לי?

נסה לדמיין, אם תוכל, שאחת מתוכנות אלו מותקנת במחשב שלך. מה ניתן לעשות?

תחילה, בדוק אם יש תוכנות חדשות כלשהן בתפריט **התחלה** או **סרגל המשימות**. חפש גם קיצורי דרך על שולחן העבודה. אם אתה יודע להשתמש בסייר Windows, חפש בתיקיה Program Files\ כדי לאתר תיקיות תוכנה שאינך מכיר. זכור שניתן לראות את התאריך בה הותקנה תוכנה על ידי בדיקה בתיבת הדו-שיח **מאפיינים** של התיקיה המתאימה (לביצוע, לחץ לחיצה ימנית על שם הקובץ, ולחץ על **מאפיינים** בתפריט שיוצג לפניך).

אם התגלתה תיקיה חשודה, פתח אותה ולחץ לחיצה כפולה על קובץ Readme.txt או קבצים דומים, כדי לקרוא על מהות התוכנה. או, תוכל להריץ קובץ EXE בתיקיה.

אם עדיין אינך מבין מה התוכנה, מחק את התיקיה באמצעות סייר Windows. **אך אל תנקה אותה מסל המיחזור;** אתה עלול לגלות מאוחר יותר שזו תוכנה שאתה צריך, אך לא זיהית אותה.

באותו זמן, חשוב היטב למי היתה גישה למחשב שלך.

אם אתה על רשת מחשבים במשרדך, צא מתוך הנחה שמנהל המערכת יכול לתעד את כל מעשיך (וזה נכון). למרות זאת, עדיין משתלם לחפש תוכנות לא רצויות.

מניעה היא עדיין התרופה הטובה ביותר

כדי שמישהו יצותת לך, הוא חייב להיות בעל גישה למחשב שלך כדי להתקין, להגדיר, ולהשתמש בתוכנת הציתות. זה קורה בעת שיש לו גישה פיסית, או, לעיתים נדירות, באמצעות חיבור דואר אלקטרוני המכיל סוס טרויאני.

אם אינך יכול לשלוט על הגישה הפיסית למחשב שלך, התקן הגנה באמצעות סיסמה (ראה פרק 3), או גרום לחוסר יכולת הפעלה פיסית של המחשב (ראה פרק 2), בהיעדרך.

ניתן להימנע מהצמדות ותוכנות סוס טרויאני של דואר אלקטרוני על ידי אי-הורדה והרצת תוכנות המצורפות לדואר אלקטרוני. תוכנות סוס טרויאני עלולות להיות גם על דיסקטים, כך שעליך להקפיד עם דיסקטים שקיבלת מאחרים.

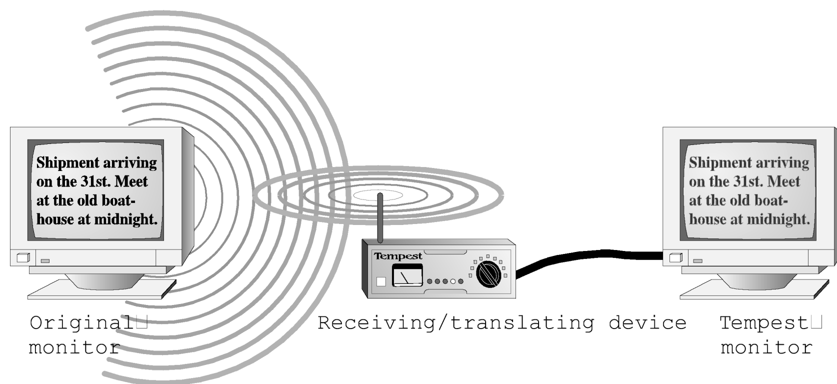
ריגול היי-טק עם TEMPEST

TEMPEST היא מערכת המאפשרת ציתות אלקטרוני על המחשב שלך. באמצעות TEMPEST, ניתן לראות מה מוקרן על צג המחשב שלך מרחוק, ללא חיבור לקו טלפון.

TEMPEST אפשרית כיון שכל התקן חשמלי או אלקטרוני יוצר קרינה אלקטרומגנטית, בדומה למשדר רדיו. תלוי בחוזקה ובאופייה, קרינה כזאת יכולה לעבור מרחקים ארוכים, אף שהיא נחלשת ככל שהמרחק גדל.

יש מכשירים מיוחדים הניתנים לכיוון לתדר המתאים, כדי לקלוט קרינה שמקורה מצג מחשב. ניתן גם להשתמש בקרינה זו כדי לשחזר את תוכן המסך ששידר אותה. תרשים 12.5 הוא תיאור מופשט של אופן הפעולה של TEMPEST.

המומחים אינם אחידים בגישתם לריגול מעין זה. חלקם טוענים שבמרחב בו אנו חיים, יש כל כך הרבה קרינה אלקטרומגנטית (טלפונים ניידים, שלט לטלוויזיה ולווידאו, טלוויזיה ומכשירי חשמל אחרים) שהיכולת לזהות מכל "הרעש" הזה את הקרינה ממסך המחשב נמוכה ביותר עד בלתי ניתנת להשגה.



תרשים 12.5 ניטור באמצעות TEMPEST

הדרך היחידה למנוע ממישהו לרגל אחריך באמצעות TEMPEST היא לסוכך על המסך שלך עם מה שמכונה **Faraday Cage**. זו היא מערכת תילי פלדה ו/או מוטות הסופגים את קרינת הצג.

למרות שיש להניח שלעולם לא תיאלץ לטפל בריגול TEMPEST, עליך לדעת שהוא אפשרי. מצד שני, ייתכן שתוך מספר שנים הציוד הייעודי הנדרש לקליטה והמרת הקרינה של צגי מחשב ייהפך לשכיח. אם זה יקרה, הבה נקווה שגם ציוד הסיכוך יהיה נפוץ באותה מידה.

האקרים ודברים אחרים שאינם בשליטתך

לא משנה באיזה אמצעי זהירות תנקוט, יש מספר מרכיבים של חטטנות ובילוש שאינם בשליטתך. זה כולל סוגי פריצה שונים (על ידי האקרים), והאזנה לקווי התקשורת.

בעיקרון, פריצה למחשב (על ידי האקרים) היא מאפיין של פעילות מקוונת. האקרים ינסו לאתר או לנחש את סיסמת ההתחברות שלך לספק האינטרנט, או לאתר שלך. לא ניתן לעשות הרבה כנגד זה, מעבר לשימוש בסיסמה קשה לפענוח והחלפתה על בסיס קבוע.

המיטב שתוכל לעשות כנגד תוכנות סוסים טרויאניים כבר נידון:

- אל תוריד ותריץ תוכנות המוצמדות לדואר אלקטרוני.
- בדוק כל תוכנה שנמסרה לך על גבי דיסקט בקפידה.
- היה בטוח במקור שלך בעת הורדת תוכנה מהאינטרנט.
- השתמש בתוכנות Norton Anti-Virus או McAfee VirusScan לניטור דואר אלקטרוני והורדות.

אם אתה רוצה לשמור או לשלוח מידע רגיש באמצעות דואר אלקטרוני, הצפן אותו. ודא שכל נמען למידע כזה מבין את ההצפנה, יש בידיו את הסיסמה או המפתח המתאים, וגם מבין את אופיו הרגיש של המידע.

התעדכן בנוגע לווירוסים חדשים, האקרים, ניטור עובדים ואיומים אחרים. האתרים הבאים מספקים מידע על נושאים מקוונים ולא-מקוונים:

- Anonymity on the Internet: http://www.dis.org/erehwon/anonymity.html
- CyberTimes (New York Times technology news online): http://www.cybertimes.net/yr/mo/day/tech/indexcyber.html
- Cypherpunks: ftp://ftp.csua.berkeley.edu/pub/cypherpunks/Home.html
- Electronic Privacy Information Center (EPIC): http://www.epic.org/
- The Privacy Page: http://www/privacy.org

עתה הגיעה העת לעיין בכמה דברים **שכן** ניתן לשלוט עליהם באמצעות סיכום והרחבת נושאים שדנו בהם כבר בעבר. פרק 13 יציג מספר דרכים נוספות להחיל את מה שכבר למדנו ועוד כמה כלים ותחבולות להגנה על הפרטיות.

פרק 13



סיכומים, אמצעים ופתרונות

מה בפרק:

- כאשר מישהו יודע את סיסמתך
- בעת קניית מחשב חדש
- להערים על האינטרנט
- פרידות והאינטרנט
- עוד כלי פרטיות
- משאבי פרטיות אלקטרוניים

פרק זה הוא בחלקו סיכום, ובחלקו מבט רענן על מידע ויישומים שימושיים. כאן תוכל לבחון מה אפשרויותיך אם מישהו משיג או מנחש את סיסמתך, ואף מספר דברים שעליך לעשות בעת רכישת מחשב חדש.

כמו כן נבקר באינטרנט שנית, ונלמד כיצד להשתמש במספר דברים שלמדנו בעבר (וכמה שטרם למדנו) כדי להערים על כל אתרי האינטרנט שכל כך מנסים להשיג מידע אישי אודותיך. בהקשר זה, גם נראה כיצד לשמור את המידע שלך מחוץ לתיקיות מקוונות - ואיך להסירו מהאינטרנט אם הוא כבר שם. נסיים בעיון במקורות מקוונים ולא מקוונים על פרטיות.

מישהו יודע את סיסמתך?

מה יקרה אם מישהו ינחש או ישיג את סיסמתך? כפי שנידון בפרקים קודמים, זה יכול להיות אסון, כיון שסיסמתך מאפשרת גישה לכל מעשיך הנוכחיים והעתידיים; מדובר בתחום רחב!

שחזור סיסמה

העדות הראשונה שמישהו השיג את סיסמתך היא כאשר הסיסמה אינה עובדת - ואז יש להניח שהנוכל שינה אותה. במקרה זה תיאלץ לגלות את הסיסמה החדשה לפני שתוכל לגשת למחשב שלך עצמך. כדי לעשות זאת, ייתכן שתוכל להשתמש בתוכנת פיצוח/אחזור סיסמאות כגון 007 Password Recovery (נמצאת בתקליטור המצורף לספר זה).

שחזור סיסמאות מקוון

אם זה אינו עובד או לא מעשי, תיאלץ לבקש עזרה חיצונית. אם מדובר רק בסיסמאות של ספק אינטרנט, שירות מקוון, או אתר אינטרנט, התקשר לשירות תמיכת לקוחות מייד, הסבר מה קרה, ובקש סיסמה או חשבון חדשים. גורמים אלה יכולים לתת לך סיסמאות חדשות לחשבון שלך.

שחזור סיסמאות של קבצים ותוכנות

אם מדובר בסוג אחר של סיסמה, עליך להתחבר לתוכנה או הקובץ האמורים, ולשנות את הסיסמה. אם אינך מצליח להיכנס לתוכנה או לקובץ, קיימות מספר אפשרויות. הראשונה היא לנחש מי גנב לך את הסיסמה. אם אתה חושד במישהו, נסה לנחש סיסמאות האמורות להתאים לו.

אם זה לא עובד, תוכל לנסות לפתוח את הקובץ עם יישום אחר מזה שיצר אותו ולנסות להעתיק את תוכנו. הבחירה הטובה ביותר לכך היא Notepad. עם אמצעים אלה תיאלץ לעבור דרך לא מעט נתונים חסרי משמעות עד שתוכל לראות את המידע האמיתי בקובץ.

תוכנות שחזור סיסמאות

הברירה הבאה היא לפנות לתוכנות לשחזור סיסמאות (הידועות גם כמפצחי סיסמאות). ישנן מספר תוכנות שיתופיות מתמחות לפיצוח סיסמאות. ביניהן יש כאלו המשחזרות או עוקפות סיסמאות בארכיבי ZIP או ארכיבים אחרים, כמו גם קבצים שנוצרו על ידי Word, Outlook, Excel ויישומים אחרים.

כמה תוכנות כאלו זמינות מ-Elcomsoft ב-http://www.elcomsoft.com. כמו כן תוכל לחפש תוכנות שיתופיות נוספות מסוג זה על ידי ביקור ב-Download.com

ו-Shareware.com (http://www.download.com ו-http://www.shareware.com בהתאמה) וחיפוש עם מילות המפתח **Password recovery**, ו-**Password Crack**.

האפשרות האחרונה לגבי קבצים

אם סיסמת קובץ או תוכנה שונתה ואינך יכול לנחש או לפרוץ אותה, מומלץ למחוק את הקובץ כך שגם הנוכל לא יוכל לגשת אליו שנית. ניתן לעשות זאת מסייר Windows.

סיסמאות Windows ומערכות הפעלה

כפי שצוין במקום אחר, ניתן לעקוף סיסמאות Windows או מערכות הפעלה על ידי אתחול מדיסקט מערכת הפעלה (דיסקט מערכת הפעלה הוא דיסקט שכולל קבצי מערכת ואתחול DOS).

סיסמאות אתחול

אם מישהו שינה את סיסמת האתחול שלך (ראה פרק 3), תיאלץ לנסות לנחש את הסיסמה או למצוא מומחה שיסיר עבורך את הסיסמה.

במקום העבודה

אם הסיסמה שלך נפרצה במקום העבודה, עליך להכין מראש תוכנית פעולה. אם אין לך תוכנית פעולה עקוב אחר השלבים הבאים:

- שנה את סיסמתך (אם ניתן).
- התקשר למנהל המערכת.
- חפש קבצים חדשים, חסרים או ששונו במערכת שלך.

תוכל גם לשגר הודעה לכל משתמשי הרשת שסיסמתך נפרצה, ולהתעלם מכל דואר אלקטרוני המגיע ממך שאינו מתאים לאופייך.

בבית

אם סיסמתך נפרצה בבית, שנה אותה מייד (שוב, אם ניתן) ואחר כך:

- ❖ בדוק קבצים ששונו, חסרים או חדשים.
- ❖ שנה את כל סיסמאותיך במערכת ואת הסיסמאות המקוונות.
- ❖ שלח דואר אלקטרוני לכל מי שאתה מכיר והסבר להם את המצב ובקש שיתעלמו מכל דואר אלקטרוני המגיע ממך והנראה להם מוזר.



אם נדרש, התקן תוכנת תזכורות שתזכיר לך להחליף סיסמה כל 30 יום.

מניעה היא עדיין התרופה הטובה ביותר

עם קצת מזל, לא תצטרך לדאוג לכל הנאמר לעיל, כיון ששינית את סיסמתך על בסיס קבוע.

קנית מחשב חדש

במוקדם או במאוחר תחליף את המחשב שלך - או שיחליפו לך אותו. זה עשוי לקרות עקב שינוי במקום העבודה, החלפת רכיב או דיסק קשיח, או שדרוג למערכות החדשות והמהירות יותר בבית או במשרד הביתי.

בעת רכישת מחשב חדש, ישנם מספר שיקולים הכרוכים בשמירה על הפרטיות. אלה אינם קשורים במחשב החדש, אלא דווקא במחשב הישן.

אם לא מכרת או נתת את המחשב הישן לאדם מוכר (ואולי גם לא במקרה כזה), אין לך כל מושג מה יהיה יעדו או מי ישתמש בו. בין אם תרמת או מכרת את המחשב שלך - בשני המקרים זה לא משנה. כל מה שהשארת על הדיסק הקשיח הולך עם המחשב.

מאחר ואינך יודע מי ישתמש במחשב הישן שלך, סביר להניח שישתמש בו אדם המסוגל לאתר ולשחזר קבצים. תמיד נקוט צעדים מתאימים למזער את הסיכוי שמידע יגיע לידיים הלא נכונות, כמתואר בעמודים הבאים.

קח מה ששלך

הדבר הראשון שעליך לעשות הוא להעתיק את קבציך האישיים - מסמכים, תמונות, קבצי נתונים, ותוכנות - על מדיה מתאימה כלשהי (זכור: ניתן להעתיק תיקיות שלמות אם נדרש). או שתשלח קבצים באמצעות דואר אלקטרוני לכתובת דואר אלקטרוני אחרת.

כדי להאיץ את הליך ההעתקה, השתמש באפשרות **הזז** וגרור קבצים נבחרים באמצעות סייר Windows כדי להעתיק את קבציך על דיסקטים או דיסקים ניידים אחרים. פעולה זו מוחקת קבצים לאחר הזזתם. כדי להגיע לאפשרות **הזז**, לחץ לחיצה ימנית על הקובץ, וגרור אותו לדיסקט/דיסק/תיקיית יעד. לאחר שביצעת זאת, שחרר את לחצן העכבר הימני. יופיע תפריט ובו מספר אפשרויות, ביניהן **הזז לכאן.** אם תוכנת הדואר האלקטרוני שלך מוגדרת לשמור העתקים של דואר יוצא, זכור שהיא גם שומרת הצמדות. או שתבטל אפשרות זו, או הקפד למחוק העתקים של דואר יוצא.

נקה אותו

לאחר שהעתקת את כל הקבצים והתיקיות ליעדם הרצוי, מחק אותם (אם לא השתמשת באפשרות **הזז).**

בנוסף, הרץ תוכנה המנקה קבצים מיותרים, כגון McAfee Uinstaller (הכלול ב-McAfee Office 2000) או Norton CleanSweep 2000. זה ימחוק קבצים חסרי ערך עבור המחשב או היישומים - ובאותו זמן ייפטר מקבצי אינטרנט וקבצים זמניים המכילים מידע עליך ופעילותך.

לאחר שמחקת קבצים מיותרים וקבצים שהעתקת, עליך לבצע עוד צעד אחד: נגב את שטח הדיסק המחוק לחלוטין בעזרת אחד הכלים המסחריים המיועדים לכך - Norton Wipeinfo (המגיע עם Norton Utilities 2000) או McAfee Office 2000. בכך תבטיח שאיש לא יוכל לאחזר את קבציך המחוקים.

סיסמאות

אם הגדרת סיסמאות מערכת כלשהן, שנה אותן למשהו שלא תשתמש בו שנית במקום אחר. עליך לעשות זאת כיון שקובץ הסיסמאות שלך עלול להישמר על ידי Windows וניתן לגשת אליו באמצעות כלי תוכנה מתאים. כך, לא תשאיר רמזים לסיסמאות העשויות להיות פעילות במקום אחר.

להערים על האינטרנט

בפרקים 9 ו- 11, ראית כמה קל שמידע עליך יזלוג לאינטרנט. המלצתי אז לשמור את שמך ומידע אישי מחוץ לאינטרנט כך שלא תמלא טפסים ותענה על פרטים אישיים בעת שיטוטך באינטרנט.

אולם, יותר ויותר מפרסמים, חנויות, ואחרים יוצרים כדאיות באמצעות הנחות, שיטות של נקודות ותמריצים מקוונים נוספים. כמובן, שאם ברצונך להירשם לשירות כלשהו, להשתתף בסקר מקוון, בתחרות, או לקנות בחנות מקוונת, תיאלץ למסור מידע אישי.

תוכל להשתמש במיגוון טכניקות ליצירת חסימה בינך לאינטרנט ולמזער את כמות המידע האישי שתספק. ניתן להשתמש בשרתי Proxy (ראה פרק 11) ולספק מידע מטעה (מספר טלפון שגוי, והטעיות דומות למידע אחר הנדרש ממך).

ניתן גם ליצור כתובות דואר אלקטרוני חד פעמיות באתרי דואר אלקטרוני באינטרנט (ראה פרק 10) כך שזרים לא יוכלו לגשת לכתובות הדואר האלקטרוני הקבועות שלך.

אם אתה משתמש בפורומים מקוונים, זכור שאוזניים לכותל - וגם זיכרון! כל דבר שתשים שם ניתן להעתקה ולשיתוף, כך שרצוי להשתמש בכתובת דואר אלקטרוני חד-פעמית לצורך דואר של פורומים.



בכל סוג של דואר אלקטרוני בו תשתמש, זכור להסיר את שמך המלא מכותרות From (מ...) ו- Reply-To (מענה ל...). כך שאיש לא יוכל לזהות אותך לפי מקור הדואר האלקטרוני שלך, אלא כמובן, אם הוא מכיר אותך היטב.



כאשר אתה נרשם לקבלת כתובת דואר אלקטרוני זמנית, אל תיתן את שמך האמיתי, וזכור שלא להכניס את שמך וכתובתך לרשימה במדריך של שירות הדואר האלקטרוני.

מעבר לכך, יש שירות די חדיש באינטרנט המחזיק את נתוניך הדמוגרפיים במעין קרן נאמנות ומשתף בה שותפי אינטרנט נוספים. השורה התחתונה היא שאתה נדרש למלא שאלונים מקוונים בתדירות נמוכה יותר, ואתה מקבל תוכן אינטרנט יותר מותאם לצרכיך האישיים.

רגשותיך בנוגע לכך הם עניינך האישי. אך אם ברצונך לבדוק אתר אחד כזה, בקר באתר nCognito ב- http://www.ncognito.com.

כמה הערות על מדריכי כתובות דואר אלקטרוני באינטרנט

מדריכי כתובות דואר אלקטרוני באינטרנט הם כלים שימושיים אם אתה מחפש כתובת דואר אלקטרוני של מישהו או רוצה שימצאו את שלך. אם אינך רוצה שכתובת הדואר האלקטרוני שלך תתגלה, מדריכי כתובות דואר אלקטרוני הם מטרד. אנשים שאינך רוצה לשמוע מהם יכולים להתקשר אליך, כמו גם אלה השולחים דואר זבל (Spammers).

הרחקת שמך ממדריכי כתובות דואר אלקטרוני באינטרנט

כדי לשמור ששמך וכתובת הדואר האלקטרוני שלך לא יוכנסו למדריכי כתובות דואר אלקטרוני באינטרנט, פעל כדלקמן:

- השתמש בכתובת דואר אלקטרוני זמנית, כאשר שמך מוסר מהכותרות בעת ביצוע שליחת דואר אלקטרוני או רשימות דיוור.
- השתמש בכתובות דואר אלקטרוני מפוברקות - או בכתובת הזמנית שלך - בעת רישום באתרי אינטרנט. הכתובת הזמנית כנראה תידרש כדי להירשם באתרי אינטרנט רבים הדורשים מענה-אישור לכתובת הדואר האלקטרוני שתספק בעת הרישום.
- אל תיתן את שמך האמיתי בעת שאתה נרשם באתרי אינטרנט.

חילוץ שמך ממדריכי כתובות דואר אלקטרוני באינטרנט

האם כתובת הדואר האלקטרוני שלך ושמך כבר נמצאים במדריכי כתובות דואר אלקטרוני באינטרנט? ייתכן מאוד. רוב משתמשי האינטרנט החדשים אינם מודעים למספר המקומות שאליהם עשויה להגיע כתובת הדואר האלקטרוני שלהם, והם שמים את שמם וכתובתם האלקטרונית בפורומים, בחדרי צ'ט וכדומה.

ככלל, תוכל פשוט לבקש הסרת שמך ממדריך. להסרת שמך, גש לכל מדריך דואר אלקטרוני ובחר קישור המאפשר הגשת בקשת הסרה, או כתוב לשירות לקוחות, מנהל האתר, או כתובת אחרת של איש קשר המופיעה באתר. **ייתכן שתיאלץ לבקש הסרה פעמיים ואף שלוש פעמים,** אך בסופו של דבר, כתובתך תוסר.

כלי פרטיות נוספים

ככל שגדלה הדאגה והעניין לפרטיות במחשב, כך רבים גם כלי ההגנה ואכיפת הפרטיות. חלק זה דן בכמה תוכנות מעניינות מסוג זה.

שולחי דואר אלקטרוני אנונימיים

שולחי דואר אנונימיים הם אתרים המאפשרים לשלוח ולקבל דואר אלקטרוני ללא חשיפת הדואר האלקטרוני שלך לנמענים. הדואר האלקטרוני מנותב כרגיל ישירות לכתובת הדואר האלקטרוני המסופקת בעת ההרשמה לשירות הדואר. להלן שניים מהשירותים הידועים יותר:

Integrity Remailer: http://www.remailer.integrity.org

Mixmaster: http://www.gilc.org/speech/anonymous/remailer.html

יש די הרבה כאלה באינטרנט, אך רבים קמים ונעלמים. אם תמצא שלא ניתן לאתר את האתרים הרשומים לעיל, נסה להשתמש בביטוי **anonymous remailer** במנוע חיפוש.

בדוק את פרטיות הגלישה שלך

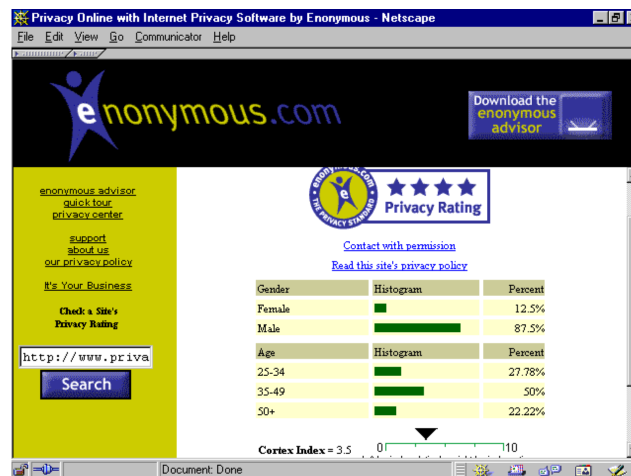
אתר זה (ראה גם בפרק 11) יציג בפניך חלק (אך לא את כל) המידע ששרת אינטרנט עשוי לאסוף אודותיך:

URL: http://privacy.net/anonymizer

היועץ האנונימי (Anonymous Advisor)

Anonymous Advisor הוא כלי תוכנה חינם, ניתן להורדה, המאפשר יצירת פרופילי-גלישה אנונימיים. זה מונע מאתרי אינטרנט לקבל מידע עליך מהדפדפן שלך. Anonymous Advisor הוא כלי מקוון, הנותן הערכת פרטיות לאתרי אינטרנט, כמתואר בתרשים 13.1.

כלי זה גם מספק הערכת פרטיות לאתר בעודך גולש בו. לבדיקת הערכה של אתר או כדי להוריד את התוכנה, בקר ב- http://www.enonymous.com.



תרשים 13.1 היועץ האנונימי (Anonymous Advisor) מעריך פרטיות אתרי אינטרנט

Fortify for Netscape

Fortify (מבצר) הוא כלי מקוון לבדיקת חוזק ההצפנה המסופק על ידי הדפדפן שלך. הוא גם מציע כלי בר-הורדה לחיזוק הצפנת הדפדפן. כתובת Fortify היא:

https://www.fortify.net/cgi/cgi-bin/ssl

Freedom (חופש)

Freedom (חופש) היא תוכנה העובדת עם הדפדפן להגן עליך משרתים אוספי-מידע על ידי שימוש בהצפנה, חסימה (בקשות מידע ו-Cookies), ועוד. היא מסייעת לחסום דואר זבל ומגבירה את פרטיות הדואר האלקטרוני שלך, צ׳טים, Telnet, ופעילות FTP.

זו היא תוכנה מסחרית. ניתן למצוא אותה בכתובת http://www.freedomnet.com

PrivacyScan (סורק פרטיות)

שירות זה סורק יותר מ- 1600 אתרים מסחריים וממשלתיים לגילוי איזה מידע אישי **אודותיך** מאוחסן בהם. זוהי תוכנה מסחרית.

שרתי Proxy

כפי שתואר בפרק 11, שרתי Proxy מאפשרים גלישה באינטרנט בלי שמידע כלשהו אודותיך ייקלט. שרתי Proxy הם מעין חוצץ. ביקוריך באתרי אינטרנט באמצעות שרת Proxy נראים לאתר כאילו אתה עצמך ביקרת. להלן כתובות של שרתי Proxy:

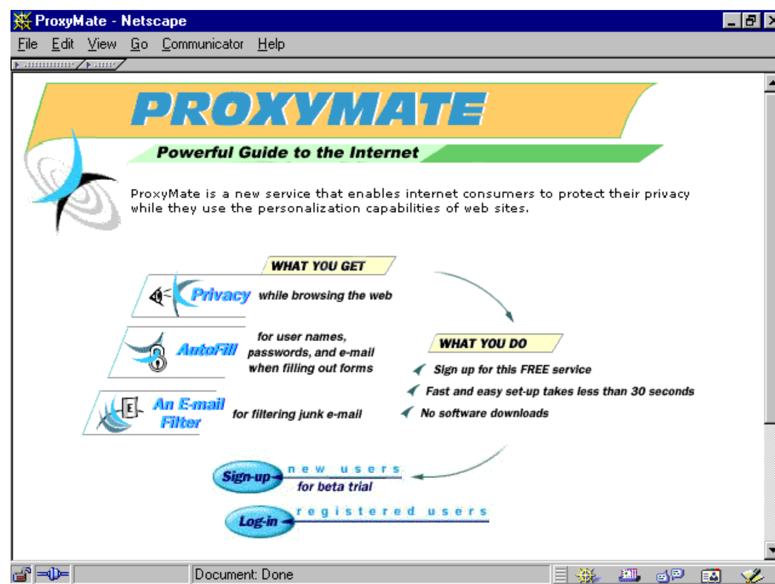
The Anonymizer: http//www.anonymizer.com

Lucent ProxyMate: http://lpwa.com:8000

מסך "ברוכים הבאים" של ProxyMate מתואר בתרשים 13.2.

מנועי חיפוש

הזכרנו מנועי חיפוש מספר פעמים. כידוע, מנועי חיפוש באינטרנט (שהם למעשה קטלוגים ברי-חיפוש או רשימות של אתרי אינטרנט) הם הדרך הטובה ביותר להשגת מידע מהר.



תרשים 13.2 ProxyMate של Lucent

אם אתה חדש באינטרנט, או לא בקיא במנועי חיפוש, להלן רשימה של מנועי החיפוש המקובלים:

AltaVista: http://www.altavista.com

AskJeeves: http://www.askjeeves.com

Exite: http://www.exite.com

Infoseek: http://www.infoseek.com

LookSmart: http://www.looksmart.com

Lycos: http://www.lycos.com

Search.com http://www.search.com

SNAP: http://www.snap.com

Webcrawler: http://www.webcrawler.com

Yahoo: http://www.yahoo.com

ורשימה (חלקית) של מנועי חיפוש ישראליים:

http://www.nana.co.il

http://www.walla.co.il

http://www.zooloo.co.il

http://www.iol.co.il

http://www.tapuz.co.il

http://www.netking.co.il

פרטיות, משאבים

ספר זה, וארגונים התומכים בפרטיות הופיעו כיון שאנשים רבים מודאגים מהאופן בו ניתן להשתמש במחשבים האישיים לחדירה לפרטיות בבית ובעבודה. להלן רשימה של כמה מארגונים אלה.

Anonymity On The Internet

אתר זה מספק מה שנראה כאין סוף קישורים למקורות מידע על פרטיות, משאבים ומידע שימושי נוסף. כתובתו:

http://www.dis.org/erehwon/anonymity.html

Center For Democracy And Technology-CDT

ארגון המגובה על ידי תעשיית המחשבים/אינטרנט, CDT הוא ממקורות הפרטיות הטובים באינטרנט. כתובתו:

http://www.cdt.org

Cypherpunks

ארגון לפרטיות באמצעות הצפנה. כתובת:

ftp://ftp.csua.berkeley.edu/pub/cypherpunks/home.html

Electronic Frontier Foundation (EFF)

ארגון בנושאי חופש הדיבור, פרטיות, וזכויות הפרט. כתובת:

http://www.epic.org

The Privacy Page

http://www.privacy.org

Privacy Rights Clearinghouse

ארגון זה מקדם גישת מחשב שקולה והיגיון בריא לשמירה על הזכות לפרטיות. באתר יש מידע רב ועצות שימושיות. כתובת:

http://www.privacyrights.org

PrivacyTimes

עיתון של הענף המספק מידע רב לצרכנים. תרשים 13.3 מראה כמה כותרות שהיו בו לאחרונה.



תרשים 13.3 עיתון PrivacyTimes

יש עוד כלים, טכניקות, ומשאבים בנושא הפרטיות הזמינים במקוון ובלא מקוון. אולם, מה שראית בספר זה מייצג את הטווח כולו. שלב את מה שלמדת עם גישותיך שלך לשמירה על פרטיות ותהיה מאובטח.

הנספחים הבאים מכילים מידע שימושי והפניות. מעבר למידע המסופק לך בספר זה, המלצתי היא לנקוט בכל אמצעי הנדרש כדי לשמור על פרטיותך.

נספח א'



מוצרים ואתרים המוזכרים בספר

שים לב: האינטרנט דינמית והכתובות יכולות להשתנות.

007 Password Recovery and 007 Stealth Activity Monitor (SAM)

IOPUS Software: http://www.iopus.com

Aladdin Expander

Aladdin Systems: http://www.aladdinsys.com

The Anonymizer

The Anonymizer: http://www.anonymizer.com

AutoShutdown

Barefoot Productions: http://www.barefootinc.com

Black Magic

Download and other information available via a search at:
http://www.download.com

Cookie Crusher

The Limit Software, Inc.: http://www.thelimitsoft.com

Cyber Patrol

The Learning Company: http://www.microsys.com/business

Digital Certificates

GlobalSign: http://www.globalsign.net/prod/

VeriSign: http://www.verisign.com

Dr Solomon□s Anti-Virus

Dr Solomon□s On-Line: http://www.drsolomons.com

E-Cash

First Virtual Bank: http://www.netchex.com/index.html

Elcomsoft

Application-specific password recovery programs: http://www.elcomsoft.com

E-Mail Directories

AnyWho: http://www.anywho.com

Bigfoot: http://www.bigfoot.com

E-Mail Directories (continued)

Internet Address Finder: http://www.iaf.net

Infospace: http://www.infospace.com

Switchboard: http://www.switchboard.com

Lycos Who Where: http://www.whowhere.com

World E-Mail Directory: http://www.worldemail.com

Yahoo□s People Finder: http://www.four11.com

E-Mail Programs

BeyondMail: http://products.banyan.com/products/download.html

Eudora: http://www.eudora.com

Pegasus: http://www.pegasus.usa.com

Encrypted Magic Folders (EMF)

PC-Magic Software: http://www.pc-magic.com

Enonymous

Privacy-rating Web site and software tool: http://www.enonymous.com

Finger Server

Finger Gateway with Faces: http://www.cs.indiana.edu:800/finger/gateway

Fortify

An online tool for testing the strength of encryption provided by browsers: https://www.fortify.net/cgi-bin/ssl

Freedom

Commercial program that blocks Web servers from getting information from your browser and system: http://www.freedomnet.com

McAfee Guard Dog, Office 2000, and VirusScan

McAfee: http://www.mcafee.com

McAfee Guard Dog: http://www.mcafee.com/products/default.asp

McAfee Office 2000: http://store.mcafee.com/product.asp?productID=89 (Available in US & Canada ONLY)

McAfee VirusScan Deluxe: http://www.mcafee.com/centers/anti-virus

Microsoft Internet Explorer

The Internet Explorer Home Page:
http://www.microsoft.com/windows/ie/default.htm

Miscellaneous

Anti-Spam Tips: http://kryten.eng.monash.edu.au/gspam.html

Coalition Against Unsolicited E-Mail (CAUCE): http://www.cauce.org/

Lamers on the Net: http://phobos.illtel.denver.co.us/pub/lamers

The Make-Money-Fast Hall of Shame: http://ga.to/mmf

Information about Cookies: http://www.cookiecentral.com

Electronic Communications Privacy Act text:
http://www.lawresearch.com/v2/Ctprivacy.htm

Netscape NetWatch (Enables you to control what types of pages are viewed with your Netscape browser only. This page provides complete information, site rating information, and interactive setup.):
http://home.netscape.com/communicator/netwatch

nCognito

Web tool for anonymous but interactive surfing: http://www.ncognito.com

Netscape

Netscape NetCenter Download and Upgrade Page:
home.netscape.com/computing/download/index.html

Norton Computing Products from Symantec: AntiVirus 2000, CleanSweep, Internet Security 2000, Secret Stuff, SystemWorks 2000, Unerase, and Norton Utilities 2000/Norton Utilities 8

Symantec Worldwide Home Page: http://www.symantec.com

Norton AntiVirus 2000: http://www.symantec.com/nav/nav_9xnt

Norton CleanSweep: http://www.symantec.com/sabu/qdeck/ncs

Norton Internet Security 2000: http://www.nortonweb.com/nis/1033/index_nc.html

Norton SystemWorks 2000: http://www.symantec.com/sabu/sysworks/index.html

Norton Computing Products from Symantec: AntiVirus 2000, CleanSweep, Internet Security 2000, Secret Stuff, SystemWorks 2000, Unerase, and Norton Utilities 2000/Norton Utilities 8 (continued)

Norton Unerase: http://www.symantec.com/nu/index.html

Norton Utilities 2000: http://www.symantec.com/nu/index.html

Norton Utilities 8: http://www.symantec.com/nu/index.html

Online Services

AOL: http://www.aol.com

CompuServe: http://www.compuserve.com

DELPHI: http://www.delphi.com

Prodigy: http://www.prodigy.com

PKZIP

PKWARE, Inc.: http://www.pkware.com

Pretty Good Privacy (PGP)

PGP Home: http://www.pgp.com

Download site (for International Version):
http://tucows.netvision.net.il/security95.html

PGP Front Ends: http://home.earthlink.net/~rjswan/pgp or
http://web.mit.edu/network/pgp.html

Privacy Resources

Anonymity on the Internet: http://www.dis.org/erehwon/anonymity.html

Center for Democracy and Technology (CDT): http://www.cdt.org

CyberTimes (New York Times technology news online):
http://www.cybertimes.net/yr/mo/day/tech/indexcyber.html

Cypherpunks: ftp://ftp.csua.berkeley.edu/pub/cypherpunks/Home.html

Electronic Frontier Foundation (EFF): http://www.eff.org

Electronic Privacy Information Center (EPIC): http://www.epic.org

The Privacy Page: http://www.privacy.org

Privacy Rights Clearinghouse (PRC): http://www.privacyrights.org

complete Analysis of your Internet Connection: http://privacy.net/anonymizer

Privacy Scan

A service that searches more than two dozen online databases for information about you: http://www.privacyscan.com

Private Bookmarks

Webroot.Com Software: http://www.webroot.com

Private File

Aladdin Systems: http://www.aladdinsys.com/privatefile

Proxy Servers

Anonymizer: http://www.anonymizer.com

ByProxy: http://www.besiex.org/ByProxy/index.html

MagnusNet: http://www.magusnet.com/proxy.html

Proxymate: http://lpwa.com:8000

Public Key Servers

BAL□s PGP Public Key Server:
http://www-swiss.ai.mit.edu/~bal/pks-commands.html

University of Paderborn PGP Public Key Server:
http://www-math.uni-paderborn.de/pgp/pks-toplev.html

Public Key Server Commands: http://bs.mit.edu:8001/pks-toplev.html

Quarterdeck Remove-It

Quarterdeck Products/Symantec:
http://www.symantec.com/sabu/qdeck/removeit-98/main98.html

Quarterdeck Zip-It

Quarterdeck Products/Symantec:
http://www.symantec.com/sabu/qdeck/zip-it/main.html

Remailers

Integrity Remailer: http://www.remailer.integrity.org

Mixmaster: http://www.gilc.org/speech/anonymous/remailer.html

Search Engines

AltaVista: http://www.altavista.com

Ask Jeeves: http://www.askjeeves.com

Excite: http://www.excite.com

Infoseek: http://www.infoseek.com

LookSmart: http://www.looksmart.com

Lycos: http://www.lycos.com

Search.com: http://www.search.com

SNAP: http://www.snap.com

Webcrawler: http://www.webcrawler.com

Yahoo: http://www.yahoo.com

ScreenLock

iJEN Software: http://www.screenlock.com

SecurePC

RSA Data Security: http://www.rsasecurity.com

Security 98

LC Technology International: http://www.lc-tech.com

Shareware Download and Information Sources

C|NET□s Download Site: http://www.download.com

C|NET□s Shareware.com: http://shareware.cnet.com

Stealth Activity Recorder & Reporter (STARR)

IOPUS Software: http://www.iopus.com

TEMPEST Surveillance

Unofficial TEMPEST Information Page:
http://www.eskimo.com/~joelm/tempest.html

Usenet Newsgroup Information and Access

AltaVista Search Engine: http://www.altavista.com

Deja News Search: http://www.deja.com/home_ps.shtml

Virus Myths

The Computer Virus Myths Home Page: http://kumite.com/myths (now found in http://www.vmyths.com/)

McAfee Virus Information Library/Hoaxes: http://vil.mcafee.com/hoax.asp

Symantec□s AntiVirus Research Center: http://www.symantec.com/avcenter

Web-Based E-Mail Services

AltaVista: http://mail.altavista.com

Excite Mail: http://mail.excite.com

Hotmail: http://www.hotmail.com

Juno: http://www.juno.com (Juno also provides free dialup access for e-mail.)

USA.Net/Net@ddress: http://www.netaddress.com

WinCode

WinSite Shareware Downloads:
http://www.winsite.com/info/pc/win3/util/wincode.zip

Windows Task Lock

Posum Software Security Technologies: http://www.posum.com

WinGuardian and Window Washer

Webroot.Com Software: http://www.webroot.com

WinGuard Impact

Rely Software: http://relysoftware.u4l.com

WinZip

Nico Mak Computing: http://www.winzip.com

נספח ב'



מילון מונחים

A

Analogue Signal (אות אנלוגי) אות המשתנה במעבר בין שני מצבים (משתנה בתדר, ברמת המתח, או בזווית הפאזה). דוגמה לכך היא בקר עוצמת הצליל של רדיו מסוג ישן (לא דיגיטלי) המאפשר כיוון רמת הצליל לכל נקודה הנעה בין גבוה לנמוך. קווי טלפון משתמשים באותות אנלוגיים, כפי שעושים רוב מערכות השידור. מערכת אנלוגית היא מערכת המשתמשת בשינויי אמפליטודה (גל) - חוזק או נפח - או תדר לנשיאת מידע.

Applet (יישומון) תוכנה הנשלחת למחשב שלך ומורצת באמצעות **דפדפן האינטרנט**. התוכנה עשויה להיכתב ב-ActiveX, או Java.

Archive (ארכיב) סוג קובץ הכולל אחד או יותר קבצים, לרוב במצב דחוס. ארכיב משמש לאחסון יעיל של קבוצות קבצים, ולאחסון קבצים בפחות שטח בידסק הקשיח. סוגי ארכיבים כוללים ARC, ARJ, ו- ZIP. ניתן להגן על רוב הארכיבים באמצעות סיסמה.

ASCII קיצור עבור **American Standard Code For Information Interchange**. ASCII הוא פורמט ספרתי סטנדרטי המשמש את רוב המחשבים להעברת מידע. יש 128 תווי ASCII סטנדרטיים (0-127), שכל אחד מהם מוקצה לתו אלפאנומרי (a...z, A...Z), מספר (0...9), תו בקרה או תו מיוחד.

ASCII Download (הורדה בשיטת ASCII) פורמט הורדה המעביר רק תווים של 7 סיביות.

Attachment (צירוף) קובץ או תוכנה המצורפת להודעת דואר אלקטרוני.

Attribute (מאפיין) מצב קובץ. מאפייני קובץ עשויים לכלול **Hidden (מוסתר)** או **Read-Only (לקריאה-בלבד)** וניתן להגדירם ב-Windows באמצעות **סייר Windows**.

B

Baud Rate התכיפות שבה אות בערוץ תקשורת עושה שינוי בין מצבים (שינוי תדר, רמות מתח, או פאזה) - כלומר יחידת מידה של מספר אירועים בודדים בשנייה אחת. Baud Rate אינו בהכרח שווה ערך לסיביות בשנייה (BPS - Bits Per Second).

Binary (בינארי) שיטת ספירה המשתמשת בשתי ספרות בלבד: 1 ו- 0. מערכת כזו משתמשת בשני מצבים (כבוי/דלוק, גבוה/נמוך, 1/0, שלילי/חיובי וכו') לייצוג מידע.

Binary File (קובץ בינארי) קובץ המאוחסן במבנה בינארי, המשתמש בספרות בינאריות, בניגוד למבנה ASCII. משמש גם להתייחסות לקבצים המאוחסנים במבנה ASCII של 8 סיביות.

Bit (סיבית) קיצור של Binary digiT. היחידה הקטנה ביותר של מידע במחשב; ערכה 1 או 0.

Bits Per Second (סיביות בשנייה) (ידוע גם כ-**Bps** או **Bit rate**) מדידת קצב העברת נתונים המבוטאת כמספר סיביות של נתונים הנשלחים בשנייה אחת. זה לא בהכרח שווה ערך ל-**Baud Rate**. כמו כן זה אינו מייצג את מספר **התווים** שנשלחו בשנייה אחת, כיון שכל תו מורכב ביותר מסיבית אחת.

BBS (ידוע גם כ-Bulletin Board System- לוח מודעות אלקטרוני) מערכת קישור באמצעות חיוג המבוססת על מחשבים אישיים או ברשת, המופעלת על ידי קבוצות קטנות או בודדים.

Board מונח עממי ל-**Bulletin Board System**. בנוסף, אזור באתר אינטרנט או שירות מקוון בו ניתן לכתוב ולקרוא הודעות ציבוריות.

Browser (גם Web Browser - דפדפן) תוכנה מיוחדת המתקשרת עם האינטרנט ומאחזרת קבצים מאתרי אינטרנט. פעולות דפדפן כוללות גם פענוח והצגת קוד **HTML** ב**דפי אינטרנט**, כולל גרפיקה וסוגים אחרים של נתונים. ניתן להשתמש בדפדפן גם לטיפול **בדואר אלקטרוני, קבוצות דיון וצ'ט.**

Bulletin Board System (לוח מודעות אלקטרוני) - ראה **BBS**

C

Capture (לכידה) אחסון טקסט או חומר אחר שמערכת מרוחקת מציגה במחשב שלך.

Character (תו) (גם **Word ,Data word**) אות, מספר, רווח, סימן פיסוק, סמל, או תו בקרה; כל מידע שניתן לאחסן ב- 1 byte (בית אחד). ייצוג מידע זה מקודד בספרות בינאריות.

Character Set (ערכת תווים) כל התווים הניתנים להצגה, הדפסה, אחסון, ו/או שידור באמצעות מחשב מסוג מסוים או מחשב מסוים.

Characters Per Second (תווים בשנייה) (גם **Cps**) מספר התווים המשודרים כל שנייה, מבוסס על קצב **Bps** (סיביות לשנייה) ואורך התווים הנשלחים.

Chat (צ'ט) מערכת הידברות בזמן אמת לניהול שיחה באמצעות הקלדה וקריאה.

Cluster (אשכול) שטח קטן על דיסק המחשב המוקדש לאחסון כמות מסוימת של נתונים. מספר אשכולות יכולים להוות **סקטור (Sector)** וסקטורים מקובצים ב**ערוצים (Tracks)** על הדיסק.

CMOS Settings (הגדרות CMOS) מונח כללי לכל הגדרות החומרה, הניתנות לשינוי, כגון: זמן, גודל זיכרון, סוגי דיסקים, וכן הלאה. הגדרות אלה לרוב נגישות על ידי לחיצה על מקש, או צירוף מקשים, בעת אתחול מחשב. רוב המחשבים מספקים אמצעים להחלת הגנת סיסמה על המערכת בעת האתחול באמצעות הגדרות CMOS.

Command (פקודה) הוראה או ערכת הוראות המורות לתוכנה לבצע פונקציה מסוימת או פעולה. ניתן להקליד פקודות או לבחור אותן מתפריט.

Communication Software (תוכנת תקשורת) תוכנה ייעודית שתפקידה לאפשר תקשורת נתונים בין מחשבים.

Configuration (תצורה) הגדרות ייחודיות מותאמות של חומרה, או בחירת הפרמטרים והפעלה של תוכנה.

Control Character (תו בקרה) תו לא מודפס שמשודר על ידי המחשב לציוד היקפי כמו מדפסת, מודם וכדומה. לדוגמה, תו בקרה הנשלח למדפסת מקדם את הדף שורה, מוציא את הדף מהמדפסת וכן הלאה.

Cookie (עוגיה) שורת מידע ששרת אינטרנט מניח בקובץ על הדיסק הקשיח שלך. ה-Cookie מכיל מידע על ביקוריך בעבר באתר אינטרנט, ומידע נוסף כגון זיהוי המשתמש (ID) וסיסמה.

D

Data (נתונים) מידע מסוג כלשהו. כתובות הן נתונים; כך גם שמות, או קבוצות מספרים (**Data** היא צורת רבים של המילה הלטינית **Datum**, ומשמשת ליחיד ולרבים כאחד).

Database (מסד נתונים) מסד נתונים מקוון הוא אוסף מאורגן של מידע קשור המאוחסן בצורת קבצים בינאריים ו/או קבצי ASCII. מסדי נתונים מכילים טקסט, תמונה, צליל ווידיאו. קבצים אלה עשויים להיות ברי חיפוש.

Data Bits (סיביות נתונים) הסיביות המייצגות תו בודד; ככלל, 7 או 8 סיביות.

Decode (הסרת קידוד) לתרגם או להסב הודעה מקודדת או מוצפנת לטקסט "ברור".

Default (ברירת מחדל) הגדרה, הוראה, או נתון המשמש תוכנה אם שום ערך לא מוכנס או נבחר על ידי המשתמש.

Defragmentation (איחוי) הליך סידור מחדש של נתונים על דיסק קשיח או דיסקט לקיצור זמני הגישה.

Delete/Erase (מחיקה) הסרת מידע על מיקום קובץ ומידע אחר מה-FAT של דיסק מחשב, כך שמערכת המחשב אינה "רואה" את הקובץ יותר ומאפשרת כתיבת נתונים חדשים במקום שבו היה הקובץ. שים לב, זה אינו מוחק את הנתונים פיסית מהמחשב, ולכן ניתן לשחזרם.

Dial Up (חיוג להתקשרות) הליך חיוג למחשב אחד מאחר באמצעות טלפון.

Dial-up System (מערכת תקשורת באמצעות חיוג) ספק **שירות אינטרנט** (**ISP**) או **שירות מקוון** הנגיש באמצעות קווי טלפון.

Digital (דיגיטלי) מתייחס או משתמש במערכת הבינארית, במיוחד לאחסון, טיפול ושידור נתונים.

Digital Computer (מחשב דיגיטלי) כל מחשב שאתה מכיר הוא מחשב דיגיטלי.

Digital Signal (אות דיגיטלי) אות מקוטע המזוהה על ידי רמה או רמות ערכים, לרוב **דלוק** או **כבוי**, או **0** או **1**. אות חשמלי בו מידע מקודד כסדרת פולסים.

Directory (ספריה) מילה נרדפת ל-**Folder** (**תיקיה**) בדיסק של מחשב אישי.

Download (הורדה) קבלת נתונים ממחשב אחר דרך חיבור אינטרנט או שירות מקוון, או באמצעות חיבור ישיר דרך קווי טלפון או כבלי חיבור אחרים. בדרך כלל, התייחסות להורדת קבצים.

E

Electronic Mail (דואר אלקטרוני, דואל) ידוע גם כ- E-mail, דואר אלקטרוני הוא מערכת הודעות מקוונת המשמשת להעברת הודעות ממשתמש מקוון אחד לאחר. קבצי דואר אלקטרוני הם לרוב פרטיים (כלומר, נגישים לשולח ולנמען בלבד). רוב מערכות דואר אלקטרוני יכולים לטפל בקבצי טקסט ASCII וקבצים בינאריים כקבצים מצורפים (**Attachments**).

Encode (קידוד) שינוי הודעה או מסמך אחר בצורה עקבית באמצעות הצפנה.

Encryption (הצפנה) אמצעי לשינוי הודעה או מסמך אחר כדי להפוך את תוכנו לבלתי ניתן לזיהוי בתהליך **קידוד** תכולת ההודעה.

F

File (קובץ) אוסף נתונים המאוחסן כיחידה על דיסק או במקוון. קובץ עשוי להכיל טקסט, תמונה, צליל או סרט וידאו.

File Name (שם קובץ) תווית הזיהוי הניתנת לקובץ. שמות קובץ במחשב לרוב מכילים שם המורכב עד 250 תווים, אחריהן באה נקודה, ולבסוף, בדרך כלל, **סיומת** של עד שלושה תווים.

Folder (תיקיה) תיקיה מכילה מספר קבצים בדיסק הקשיח. שם נרדף ל**ספריה (directory)** במחשב.

Freeware (תוכנות חינם) תוכנה המופצת חינם, ולא נדרש לשלם עבור השימוש בה.

FTP קיצור ל-**File Transfer Protocol**, שהוא מונח כללי לשיטה המשמשת להעברת (הורדה) קבצים בין מחשב למחשב.

H

Hardware אוסף הרכיבים הפיסיים הבודדים או המורכבים של מערכת מחשב, כולל, אך לא מוגבל רק למקלדת, צג, כונן תקליטורים, מדפסת, מודם, והתקנים מחוברים או ניידים אחרים.

Hidden (מוסתר) מאפיין (Attribute) הגורם שקובץ או תיקיה יהיו בלתי נראים ליישומים.

Host System (מערכת לקוח) מושג יחסי המתייחס למערכת בה אתה משתמש. ככלל, מערכת המקבלת קריאה ממערכת אחרת (הידועה גם בשם **מערכת מרוחקת - Remote system**).

HTML קיצור של **HyperText Markup Language.** HTML היא מערכת לקידוד טקסט המציגה את הטקסט בצורה מסוימת (גודל ומידת גופן, מיקום, וכן הלאה). **דפדפני אינטרנט** מתרגמים את קוד HTML ומציגים את המידע על המסך. HTML גם משמשת להצגת **קישורים** לדפי אינטרנט אחרים, לאתרים, לתמונות, לקבצים להורדה, ועוד.

Hyperlink (היפר-קישור או בקיצור **קישור)** שורת טקסט, תמונה, סמל, או דף אינטרנט המספק קישור למשאב - דף אינטרנט אחר, קובץ, או תוכנה. היפר-קישורים מסומנים בקוד HTML, ומובילים ל-**URL** מסוים.

I

ID, Identifier, userID, username (זיהוי, מזהה, זיהוי משתמש, שם משתמש) השם לפיו אתה מזהה את עצמך לשירות המקוון, ספק האינטרנט, או אתר האינטרנט. מידע מגוון קשור לזיהוי המקוון שלך, כגון **password (סיסמה)**, פרמטרים של תצוגה, ועוד. זיהוי יכול להיות מספר, שם, או סדרת אותיות וספרות.

Input (קלט) פקודה, ערך, או נתון אחר המסופק לתוכנה או למסד נתונים על ידי משתמש מחשב או מקור חיצוני. הקלט יכול להיות לחיצה בעכבר או הקלדה במקלדת.

Internet (אינטרנט) רשת המחשבים העולמית בה המחשבים מקושרים ביניהם ובמידע שהם מכילים. זה כולל דפי אינטרנט, דואר אלקטרוני, מערכות פורומים כגון Usenet Newsgroup, והחומרה הפיסית של המחשבים והתקשורת הקושרת את מערכות המחשב יחד. שים לב שרשת האינטרנט (Web), Usenet, ודואר אלקטרוני אינם מהווים לבד את ה"אינטרנט". האינטרנט הוא שילובם של כל הגורמים האלה.

ISP (ספק שירותי אינטרנט) זה הוא קיצור של **Information Service Provider**. ISP מספק קישור לאינטרנט לאנשים פרטיים ועסקים. ככלל, ISP גם מטפל בדואר אלקטרוני עבור לקוחותיו ועשוי לאחסן דפי אינטרנט בנוסף לנתונים על כל משתמש.

K

Kilobyte (קילו-בית) (מכונה גם K). יחידת מדידה של זיכרון מחשב, המתייחסת למספר הבתים בזיכרון RAM או גודל קובץ. ערכה 1024 בתים (byte).

L

Local System (מערכת מקומית) מונח יחסי, המעיד לרוב על סוג מערכת המחשב שבשימוש, או מחשב היוצר קשר עם מחשב אחר (אשר נקרא מערכת מרוחקת [Remote System]).

M

Megabyte (מגה-בית) (מכונה גם **MB**). יחידת מדידה לזיכרון מחשב בעלת ערך של 1024 קילו-בית (Kilobyte). מתייחס למספר הבתים בזיכרון RAM, גודל קובץ, או נפח הדיסק הקשיח.

Modem (מודם) (מקור המילה **MOdulate-DEModulate**) התקן המשמש לתרגום אות דיגיטלית ממחשב לאות אנלוגית לשידור דרך קווי טלפון, ולהיפך.

N

Newsgroups (קבוצות דיון) ראה Usenet Newsgroups

O

Offline (לא מקוון) מצב בו מערכת מחשב אינה מחוברת למחשב אחר.

Online (מקוון) מצב בו מערכת מחשב מחוברת למחשב אחר; ההיפך מ-Offline.

Online Service (שירות מקוון) שירות מסחרי המספק אחד או יותר מן השירותים הבאים: תקשורת, מסד נתונים, אחסון ואחזור מידע ושירותים אחרים. לדוגמה: אתה גולש לאתר ורואה את מצב המניות בבורסה, ספק האינטרנט שלך מאפשר לך משלוח דואר אלקטרוני, רכשת ספר באתר של הוד-עמי באינטרנט - כל אלה זה שירות מקוון.

Output (פלט) מידע הנשלח ממחשב אל המסך שלו, למדפסת, לקובץ דיסק, או מחשב אחר.

P

Packet (מנה) יחידת נתונים משודרת המורכבת מתוכן (**תווים**) יחד עם מידע על מקורם, הנתיב שלהם ויעדם. קבצי נתונים של מחשב משודרים במנות כאלה באמצעות **Packet-switching networks (מערכות מיתוג מנות).**

Packet-switching networks (מערכות מיתוג מנות, מכונה גם **PSN**). מערכת תקשורת נתונים המשדרת נתונים ממחשב אחד לאחר בצורת **Packets (מנות).** זו השיטה בה עוברים הנתונים ברשת האינטרנט.

Parameters (פרמטרים) הגדרות שנבחרו על ידי משתמש מחשב ו/או מוכללות בתוכנה, המשמשים כערכים קבועים או ברירות מחדל בפעולת תוכנה.

Password (סיסמה) מחרוזת אותיות ו/או מספרים המשמשת לזיהוי משתמש באתרי אינטרנט או בעת הפעלת המחשב. שימוש בסיסמאות מונע שימוש לא מורשה במשאבים. סיסמאות אמורות להיות ידועות רק לאלה המגדירים אותן.

Power-On Password (סיסמת אתחול) (ידוע גם כ-**Boot password**, **Startup password**). סיסמה המוגדרת ב**הגדרות CMOS** המונעת מהמחשב לטעון את מערכת ההפעלה ללא הסיסמה.

Private Key (מפתח פרטי) במערכת **הצפנת מפתח ציבורי (Public key encryption)**, משמש לפענוח הודעה או מסמך אחר שהוצפן באמצעות **מפתח ציבורי (Public key)**.

Profile (פרופיל) אצל כמה ספקי שירות אינטרנט (ISP), אתרי אינטרנט, ושירותים מקוונים, ערכת **פרמטרים ברירת מחדל** ש**המערכת המארחת** משתמשת בהן כדי להידבר עם המחשב. פרופיל עשוי לכלול מידע על פרמטרים לתצוגה (רוחב מסך, צבע), תצוגת סמנים/תפריטים, ורכיבים נוספים.

סוג נוסף של פרופיל מקוון, כולל מידע על **משתמש (User)** בודד, כגון שם, מיקום, תחומי התעניינות, וכן הלאה. ככלל, המשתמש יכול לשנות את שני סוגי הפרופילים.

Program (תוכנה) ערכת הוראות המורה למחשב כיצד לבצע מטלה או מטלות מסוימות, והמעבדת פקודות וקלט.

Public Key (מפתח ציבורי) **הצפנת מפתח ציבורי (Public key encryption)**, משמשת להצפנת מסמך. לאחר ההצפנה, ניתן לפענח את המסמך רק בעזרת **מפתח פרטי (Private key)**. מפתח ציבורי נשלח על ידי מי שבידיו נמצא המפתח הפרטי. מי שמקבל את המפתח הציבורי מצפין בעזרתו מסר שרק מי שבידיו המפתח הפרטי מסוגל לקרוא.

Public key encryption (הצפנת מפתח ציבורי) שיטת הצפנה בה נדרשים שני מפתחות לקריאת מסר: **מפתח פרטי** (**Private key**) **ומפתח ציבורי** (**Public key**) .

R

Read-only (קריאה-בלבד) זה הוא **מאפיין (Attribute)** המונע שינוי קובץ על ידי יישום.

Remote System (מערכת מרוחקת) מונח יחסי להתייחסות למערכת בה אינך משתמש; ככלל, המערכת המקבלת את הקריאה (מכונה גם **מערכת מארחת - Host system**), בניגוד למחשב המבצע את הקריאה.

S

Sector (סקטור) אזור בדיסק המחשב המאחסן את כל או חלק מהנתונים בקובץ. סקטורים מורכבים לעיתים מיחידות אחסון מידע קטנות יותר הנקראות **אשכולות (Clusters)** המונחות ב**ערוצים (Tracks)** על הדיסק.

Shareware (תוכנות שיתופיות) תוכנה המופצת באופן חופשי על בסיס "נסה לפני שתקנה". אם התוכנה לטעמך וברצונך להמשיך להשתמש בה, אתה נדרש לשלם ליוצריה. בדרך כלל גרסאות Shareware מוגבלות באופן כלשהו: ל- 30 יום או שלא ניתן לעשות שימוש בכל יכולות התוכנה.

Sign on (התחברות) (ידוע גם כ-**Login, Logon**). הליך או אירוע התחברות וזיהוי המחשב שלך במערכת מחשב אחרת, או אתר אינטרנט. ככלל, הליך ההתחברות כרוך במסירת שם וסיסמה לפי דרישה.

Spam (דואר אלקטרוני זבל) סלנג אינטרנט לדואר אלקטרוני לא נדרש, הכולל ככלל, פרסום, הונאות, שידול, רמאויות וסתם... זבל.

String (מחרוזת) סדרת אותיות, ספרות, או סמלים המשמשים כקלט או פלט נתונים. מחרוזות שלא ניתנות לשימוש כאופרטורים ספרתיים ושערכן אינו משתנה הן **מחרוזות תווים (Character strings).** Franklin Robert Adams, ו- 555-1969, ו- 3-21-51 הן כולן מחרוזות תווים. מחרוזות עם ערכים מספריים קבועים הן **מחרוזות מספריות (numeric strings)**. 450.50 ו- 910234 הן מחרוזות מספריות.

Sysop (מפעיל מערכת) קיצור ל-**SYStem OPerator.** אדם האחראי על רשת המחשבים במשרד, אדם המפעיל ספק שירותי אינטרנט (ISP), או המפעיל אזור מסוים של שירות מקוון או אתר אינטרנט. במקומות בהם יש מערכות תקשורת מקומיות (LAN) התואר הוא לרוב "מנהל מערכת" (System Administrator).

System (מערכת) מונח המשמש להתייחסות לכל מחשב (והציוד ההיקפי שלו) - במיוחד מחשב המחובר למחשבים אחר, בין אם כשרת או כתחנת עבודה.

T

Telecomunications (תקשורת טלפונית) תקשורת נתונים על גבי קווי טלפון באמצעות מחשבים והתקנים נלווים.

Telecomputing (תקשורת מחשבים) ככלל, שימוש במחשב אישי להתחברות למחשבים אחרים.

Temporary Files (קבצים זמניים) קבצים הנוצרים על ידי מערכת ההפעלה או על ידי תוכנות כתמיכה במטלות מסוימות הנדרשות על ידי התוכנה. קבצים אלה נמחקים לאחר שהתוכנה סיימה לעבוד אתם, אך לא תמיד. קבצים זמניים לעיתים מספקים עקבות מפורטים על מעשיו של אדם במחשב.

Text (טקסט) כל הודעה או קובץ המורכב מ**תווי ASCII** סטנדרטיים.

Text File (קובץ טקסט) קובץ במבנה ASCII בניגוד לקובץ במבנה **בינארי (Binary).**

Track (ערוץ) אזור בדיסק המחשב שבו מאוחסן מידע, המכיל מספר **סקטורים (Sectors)**, המכילים **אשכולות (Clusters).**

Trojan horse (סוס טרויאני) תוכנה ה"נשתלת" במחשב ומשדרת משם את הפעולות הנעשות בו ו/או את הנתונים המאוחסנים בו. תוכנה זו גם יכולה לגרום נתק במחשב בו היא הושתלה על ידי מחיקת קבצים או כל נזק אחר.

U

Undelete/Unerase (ביטול מחיקה) הליך שחזור נתונים ש**נמחקו** מדיסק מחשב.

Upload (העלאת חומר) שליחת מידע למחשב אחר, באמצעות חיבור אינטרנט, שירות מקוון, או באמצעות חיבור ישיר באמצעות קווי טלפון או כבלי חיבור.

URL קיצור **Uniform Resource Locator**. URL הן ה"כתובות" שבהם משתמש הדפדפן להתקשר לאתרי אינטרנט ודפי אינטרנט. דוגמה לכתובת URL טיפוסית היא http:\\www.hod-ami.co.il

Usenet Newsgroups (קבוצות דיון) מערכת פורומים הנגישה באמצעות האינטרנט. ישנן עשרות אלפי קבוצות דיון, כל אחת ייעודית לנושא מסוים.

User (משתמש) מונח לאדם המתחבר, או משתמש באינטרנט. כמו כן, לכל משתמש מחשב באופן כללי.

V

Virus (וירוס) תוכנה או מאקרו שפעולתה לרוב הרסנית או מפריעה למערכת מחשב. ישנו מיגוון אינסופי של וירוסים (יותר מ- 50,000 ידועים), אך התוצאה הסופית זהה - הפרעה או הרס נתונים במחשב.

W

Web page (דף אינטרנט) ככלל, מסמך במבנה **HTML**, הכולל **היפר-קישורים** (ידועים גם כ**קישורים**) לדפי אינטרנט אחרים באתר זה, או לכל מקום אחר באינטרנט. דפי האינטרנט עשויים גם להכיל גרפיקה, וקישורים להפעלת תוכנות במערכת שלך, הורדת קבצים, ו/או ביצוע פעולות אחרות.

Web Site (אתר אינטרנט) אוסף **דפי אינטרנט (Web Pages)**, גרפיקה וקבצי נתונים נוספים המתארחים במחשב מחובר לאינטרנט. המחשב המארח את האתר מכונה **שרת (Server).**

Wipe (לנגב/למחוק) להסיר לחלוטין כל עקבות קובץ מחוק על ידי כתיבה על שטח הדיסק שהקובץ איכלס בעבר.

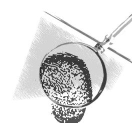
World Wide Web (ידוע גם כ-**WWW**, **web**) אוסף **אתרי האינטרנט ודפי אינטרנט** הזמינים באמצעות חיבור לאינטרנט.

נספח ג'



התקליטור המצורף

- **קטלוג HTML** - קטלוג ספרי המחשבים האינטראקטיבי של **הוצאת הוד-עמי**.
  לשם קריאת הפרקים לדוגמה יש להתקין את תוכנת Adobe Acrobat Reader אשר מצורפת בתקליטור. הוראות התקנה בהמשך.
  הקטלוג מומלץ לצפייה באמצעות Internet Explorer גירסה 5, המצורפת בתקליטור. הוראות התקנה בהמשך.
  התקנת שתי התוכנות קלה וניתנת לביצוע באמצעות קישור ישירות מהקטלוג.
- מספר תוכנות עזר שימושיות.



אם מנהל התקן כונן התקליטורים המותקן הוא 16 סיביות - ייתכן שתראה רק 8 תווים ראשונים של שם קובץ (במידה שהמקור ארוך יותר).

הסיבה: כונני תקליטורים במהירות x4 עובדים עם מנהל התקן שעבד בסביבת DOS ו-Windows 3.11 ויכול לעבוד גם עם Windows 95, למעט היכולת לזהות קבצים עם שמות ארוכים.

הפתרון: להתקין מנהל התקן 32 סיביות (אם קיים), או לקנות כונן תקליטורים חדש ולוודא שמצורף אליו מנהל התקן 32 סיביות..

קרא את קובץ ONCD שבתקליטור כדי לקבל עוד מידע לגבי התקליטור

התיקיה הרלוונטית לספר זה

(הרשימה חלקית ועשויה להשתנות)

התיקיה **Books\59297** מכילה תוכניות המוזכרות בספר וקשורות לנושא שלו.

ברוב התיקיות המכילות תוכנות בתקליטור תמצא קובץ File_id.diz או קובץ ReadMe.txt. בקבצים אלה תמצא פירוט לגבי התוכנה. מומלץ מאוד לקרוא את תוכן קבצים אלה (על ידי לחיצה כפולה עליהם) לפני ביצוע התקנה של תוכנה כלשהי מהתקליטור.

רצוי מאוד שתדע מה התוכנה עושה והאם אתה יודע בדיוק מה אתה עומד לעשות. להזכירך, הוצאת הוד-עמי אינה תומכת ואינה אחראית לכל נזק שייגרם, אם ייגרם.

אין צורך להעתיק את התוכנות לדיסק אלא רק להתקין את התוכנה הרצויה על ידי לחיצה כפולה על הקובץ בעל הסיומת EXE (בדרך כלל).

Password Recovery	Lockit
Advisor	Private BookMArks
AladdinSys	ScreenLock
AutoShutDown	Stealth Monitor
BlackMagic	Stealth Recorder
CookieCrusher	WebRoot
CyberPatrol	WinCode
EncryptedMagicFolder	Windows TaskLock
	WinGuard

התקנה - Acrobat Reader

יש להתקין תוכנה זו כדי לקרוא ולהדפיס את הפרקים לדוגמה, אליהם ניתן לגשת באמצעות **קטלוג HTML** (שהתקנתו תוסבר בהמשך). התוכנה גם מאפשרת חיפוש בעברית ובאנגלית במסמך המוצג. בנוסף, בעזרת תוכנה זו תוכל לקרוא את המסמכים שההוצאה מפרסמת באתר האינטרנט. התוכנה פועלת במערכות הפעלה
Windows 95 ומעלה!

1. לחץ על לחצן **התחל** ובחר באפשרות **הפעלה**.
2. בתיבת הטקסט הקלד את הפקודה
X:\Software\Adobe Acrobat\Arme4ENU.exe
(החלף את האות X באות המייצגת את כונן התקליטורים שלך) ולחץ על **אישור**.
3. אשף ההתקנה מתקין את הרכיבים הנדרשים. עליך ללחוץ על **Next**, **Accept** ו-**Next** פעם נוספת כדי לסיים את ההתקנה.
4. בסיום ההתקנה עשויה להופיע על המסך תיבת דו-שיח **התנגשות בין גירסאות** ומייד אחר כך להיעלם. במקומה תופיע על המסך תיבת הודעה של תוכנית ההתקנה. לחץ על **אישור** ובתיבת הדו-שיח **התנגשות בין גירסאות** ששבה להופיע לחץ על **כן**, כדי לשמור את גרסת הקובץ שלך.

קטלוג HTML

הוצאת הוד-עמי גאה לבשר על **קטלוג HTML** העושה שימוש בטכנולוגיות אינטרנט מתקדמות כדי להביא לך את המידע על ספרי המחשבים המקצועיים שלנו בלחיצת עכבר.

מומלץ לצפייה בעזרת Microsoft Internet Explorer מגירסה 5 ומעלה.

בעזרת **קטלוג HTML** תוכל:

- ✯ לעיין במידע על ספרי ההוצאה מתי שתרצה (לחיצה כפולה.... וזהו!).
- ✯ לעבור במהירות ובקלות בין הקטלוג והיישום בו אתה עובד.
- ✯ לעיין במידע על כל ספר וספר.
- ✯ לצפות ואף להדפיס פרק לדוגמה.
- ✯ לגשת במהירות, בגישה אינטואיטיבית, תוך התמקדות מהירה בספר המבוקש.
- ✯ לעיין בקטלוג בקצב אישי שלך.
- ✯ לנווט את דרכך בקטלוג ולחזור ולהתרענן בכל נושא בכל רגע.

הקטלוג מומלץ לצפייה בעזרת Internet Explorer מגירסה 5 ומעלה.

1. הכנס את התקליטור לכונן.
2. לחץ **התחל** ובחר **הפעלה**.
3. בעזרת לחצן עיון סמן את הקובץ **Setup.exe** אשר בתיקיה הראשית של התקליטור המצורף.
4. לחץ **פתח**.
5. לחץ **אישור**.

המחירון המעודכן של ספרי ההוצאה נמצא באתר האינטרנט www.hod-ami.co.il

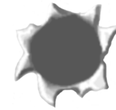


קטלוג ספרי מחשבים בהוצאת הוד-עמי

6. ודא שתקליטור הוד-עמי נמצא בכונן התקליטורים.
7. הפעל את הסמל עם הכיתוב **קטלוג ספרי מחשבים בהוצאת הוד-עמי** שעל שולחן העבודה.

מה עוד בתקליטור?

הוצאת **הוד-עמי** מפיצה תוכנות אלו כבונוס ללקוחות ההוצאה, ואינה מתיימרת לגבות תשלום עבור התוכניות המצורפות ו/או לתמוך בהם.



השימוש בתקליטור זה הוא על אחריותו הבלעדית של המשתמש. המוצרים המותקנים בתקליטור זה מסופקים באחריות החברות המייצרות אותם. הוצאת **הוד-עמי** אינה אחראית, בכל צורה שהיא, לאופן ולטיב התוכנות המותקנות.

בכל שאלה לגבי תוכנה הנמצאת בתקליטור, יש לפנות למפתחי התוכנה (כל תוכנה בנפרד) כפי שמצוין בקבצי העזרה של התוכנה המדוברת.

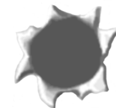
הקבצים הם גרסאות **שיתופיות** (ShareWare) **וחופשיות** (FreeWare).

גרסת ShareWare מאפשרת לך, המשתמש, לבדוק את יעילות התוכנה ואת תאימותה לעבודה אותה אתה מבצע. אם נמצאה התוכנה מתאימה לצרכיך, עליך לשלם למפתחיה תשלום סמלי (לפי הרשום בקבצי העזרה של כל תוכנה ותוכנה בנפרד) כדי לקבל רישיון מלא לשימוש בה. קבלת רישיון לשימוש בתוכנה יפתח בפניך מיגוון אפשרויות שלא עמדו לרשותך בהפעלת גרסת ה-ShareWare.

התקנת תוכנת גלישה לאינטרנט Microsoft Internet Explorer 5

תוכנית ההתקנה מזהה את גרסת מערכת ההפעלה ומתקינה את גרסת הדפדפן הדרושה. מומלץ להסיר גירסה קודמת של Internet Explorer, אם קיימת.

1. הכנס את התקליטור לכונן.
2. לחץ על לחצן **התחל** ובחר באפשרות **הפעלה**.
3. לחץ על לחצן **עיון**.
4. בחר בכונן התקליטורים בתיקיה Software\IE5 ובקובץ בשם SETUP.EXE.
5. לחץ על לחצן **פתח**. לחץ על לחצן **אישור**.
6. פעל לפי ההוראות על המסך.



לפני ביצוע שדרוג מ-Windows 95 ל- Windows 98 בעברית (זו בה התפריטים בעברית ולחצן התחל מימין שורת המשימות), יש להסיר את Internet Explorer 5. לאחר השדרוג ניתן לבצע התקנה מחדש של הגירסה המתאימה.

FontsPekan

קובץ זה יתקין במחשב 2 גופנים בעברית לשימושכם. בסיום ההתקנה יש לבצע את הפעולות הבאות:

1. לחץ על **התחל**, הצבע על **הגדרות**, ובחר ב**לוח הבקרה**.
2. לחץ לחיצה כפולה על הסמל **גופנים**.
3. פתח את תפריט **קובץ** ובחר באפשרות **התקנת גופן חדש**.
4. עבור לתיקיה **C:\FontsPekan**.
5. לחץ על לחצן **בחר הכל** (סה"כ יש בתיקיה 2 גופנים).
6. ודא שתיבת הסימון **העתק גופנים לתיקיית הגופנים** מסומנת.
7. לחץ **אישור**.
8. סגור את חלון התיקיה **Fonts**.
9. סגור את חלון **לוח הבקרה**.

כעת, מוכנים הגופנים לשימוש בכל התוכנות המותקנות במחשב שלך: Word, Excel, PowerPoint וגם בתוכנות גרפיות, כגון Paint Shop Pro ו-PhotoShop.

הגופנים נקראים Tml-JUMP ו-Tml-step ויופיעו בתחתית רשימת שמות הגופנים (בדרך כלל). הרי דוגמה שלהם:

Tml-step

אבגדהוזחטיכךלמםנןסעפףצץקרשת1234567890

Tml-JUMP

אבגדהוזחטיכךלמםנןסעפףצץקרשת1234567890

NETEX

במקום לרשום **http://www.hod-ami.co.il** פשוט רישמו **הוד-עמי** והנה אתם באתר ההוצאה.

במטרה להגיע לאתר מסוים באינטרנט, שכתובתו אינה ידועה, אנו משתמשים בדרך-כלל באחת משתי דרכים: ניחוש של כתובת האתר ו/או פנייה לאינדקס או למנוע חיפוש

שתי הפעולות הן מסורבלות וגוזלות זמן ואנרגיה מיותרים. ניחוש הכתובת מחייב הקלדה של הכתובת המלאה באנגלית בדיוק מושלם, והוא עשוי להיות הליך גוזל זמן, במיוחד כאשר לא מצליחים למצוא את האתר בניסיון ראשון או בכלל.

עם netex לא צריך לנחש כתובות או לגלוש למנועי חיפוש כדי להגיע לאתר מסוים ברשת! פשוט מקלידים את שם האתר בעברית בחלון הכתובת בדפדפן, ומגיעים אליו ישירות.

אפשרויות השימוש במערכת

גלישה ישירה לאתר על-פי שמו או על-פי נתונים הקשורים בו.

מקלידים בחלון הכתובת של הדפדפן שם של אתר או חברה או מילות מפתח הקשורות באתר (בכל סדר שהוא), ומגיעים אליו ישירות.

לדוגמה:

- ✯ מקלידים הוד-עמי או הוצאת הוד-עמי או ספרי מחשבים ומגיעים ישירות לאתר הוצאת הוד-עמי לספרי מחשבים.
- ✯ מקלידים **בנק דיסקונט** - ומגיעים ישירות לאתר של בנק דיסקונט.
- ✯ מקלידים **סלקום** או **052** - ומגיעים ישירות לאתר של חברת סלקום;
- ✯ מקלידים **עכבר העיר** - ומגיעים ישירות לאתר של העכבר;
- ✯ מקלידים **144** - ומגיעים למודיעין 144 של בזק;

התחברות למערכת הניתוב החדשה של ישראל

כל שעליכם לעשות כדי להתחבר ל-NETEX הוא להתקין תוכנה קלה וחכמה:

1. יש לסגור את כל התוכנות הפתוחות כולל הדפדפנים הפועלים.
2. מתוך סייר Windows הפעילו את הקובץ **netex100.exe** שבתיקיה X:\Software\NetEx.
3. פעלו בהתאם להוראות.

בזמן ההתקנה התוכנה מזהה את הדפדפן/ים שמותקנים במחשב, והיא תפעל עם כולם. מייד אחרי סיום ההתקנה תוכלו להתחיל לגלוש חכם ובעברית.

המערכת שקופה למשתמש, כלומר היא "מתלבשת" על הדפדפן הרגיל ואינה נראית כלל. אין צורך להפעיל אותה או לבצע פעולה כלשהי כדי להשתמש בה: פשוט מקלידים את שם האתר המבוקש בשדה הכתובת של הדפדפן, ומגיעים ישר אליו.

התוכנה אינה מפריעה לעבודה רגילה עם הדפדפן. היא נכנסת לפעולה רק כאשר מקלידים נתון שאינו כתובת אינטרנט רגילה (URL). כאשר תקלידו **www.hod-ami.co.il** תגלשו ישירות לאתר **הוצאת הוד-עמי**, בדיוק כפי שנהגתם לגלוש לפני התקנת התוכנה (ללא מעורבות המערכת). אך אם תרצו, תוכלו להקליד **הוד-עמי** בשדה כתובת ולהגיע במהירות לאותו אתר בדיוק.

תיקיה ראשית SoftWare
(רשימה חלקית ועשויה להשתנות)

הערה : תוכנות להן יש גירסה מיוחדת עבור Windows 2000 יסומנו בתיקיה ששמה מסתיים ב- 2k (למשל, בתיקיה ICQ נמצא קובץ התקנה לתוכנה זו המתאים לכל גירסאות Windows, ובתיקיה ICQ2k נמצא קובץ התקנה עבור מערכת ההפעלה Windows 2000 בלבד).

בדרך כלל לחיצה כפולה על שם הקובץ המפורט ברשימה מפעילה את תוכנית ההתקנה.

שם תוכנה	תיאור
Adobe Acrobat	תוכנה לצפייה בקבצי pdf
Clean System	מחיקת קבצי dll שאין צורך בהם
FontsPekan	גופנים בעברית
ICQ	תוכנה לתקשורת אישית באינטרנט
MIRC	תוכנת הצ׳אט הפופולרית ביותר ברשת
NetEx	תוכנה המאפשרת גלישה בעברית
Paint Shop Pro 6	תוכנה ליצירת, עיצוב ועיבוד תמונות
Power Toys	תוכניות שירות עבור Windows 9x
WinAmp	תוכנה להשמעת קבצי MP3 (מוסיקה)
WinZip	תוכנית לפריסה/דחיסה של קבצים
WordView	תוכנית לצפייה בקבצי doc



אינדקס עברי

ע

פ

צ

ק



אינדקס לועזי

האינדקס באנגלית ולכן הוא מתחיל מסוף הספר בעמוד מספר 1 ומתקדם בכיוון פנימה לספר עד לעמוד הבא.

אינדקס לועזי 

C

F

N

O

P

S

T

U